(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 946 018 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
14.03.2007 Bulletin 2007/11

(51) Int Cl.:
H04L 9/30 (2006.01)

(21) Application number: **99105099.8**

(22) Date of filing: **25.03.1999**

(54) Scheme for fast realization of a decryption or an authentication

Verfahren zur schnellen Ausführung einer Entschlüsselung oder einer Authentifizierung

Procédé de réalisation rapide d'un d'un déchiffrage ou d'une authentification

(84) Designated Contracting States:
DE FR

(30) Priority: **26.03.1998 JP 7983698**
21.08.1998 JP 23608498

(43) Date of publication of application:
29.09.1999 Bulletin 1999/39

(73) Proprietor: **NIPPON TELEGRAPH AND TELEPHONE CORPORATION**
Tokyo (JP)

(72) Inventors:
- **Takagi, Tsuyoshi,**
  c/o Nippon T.& T. Corporation
  Shinjuku-ku,
  Tokyo 163-14 (JP)
- **Naito, Shozo,**
  c/o Nippon T. & T. Corporation
  Shinjuku-ku,
  Tokyo 163-14 (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(56) References cited:
EP-A- 0 381 523
EP-A- 0 823 802
WO-A-90/02456
WO-A-98/26536

- **FRANKEL Y ET AL: "PROACTIVE RSA" , ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, VOL. CONF. 17, PAGE(S) 440-454 XP000767549 ISBN: 3-540-63384-7 * page 443, line 37 - line 40 ***
- **BRUCE SCHNEIER: "Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition" 1996 , JOHN WILEY & SONS, INC. , NEW YORK XP002201616 * page 249 - page 250 ***
- **TAKAGI T: "FAST RSA-TYPE CRYPTOSYSTEM MODULO PKQ" , ADVANCES IN CRYPTOLOGY. CRYPTO '98. 18TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 23 - 27, 1998. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1462, BERLIN: SPRINGER, DE, PAGE(S) 318-326 XP000792177 ISBN: 3-540-64892-5 * the whole document ***

EP 0 946 018 B1

Description

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention relates to a scheme for fast realization of encryption, decryption and authentication which is suitable for data concealment and communicating individual authentication in communications for a digital TV, a pay-per-view system of the satellite broadcast, a key distribution in the information distribution, electronic mails, electronic transactions, etc.

DESCRIPTION OF THE BACKGROUND ART

[0002] In recent years, in the field of communications, various types of cryptographic techniques have been proposed because the cryptographic technique can be effectively used for the protection of secrecy between communicating parties such as the concealment of information to be transmitted. The performances of such a cryptographic technique can be evaluated in terms of the security level of cryptosystem and the speed of encryption/decryption. Namely, the cryptosystem for which the security level is high and the encryption/decryption speed is high is a superior cryptosystem.

[0003] Among such cryptographic techniques, there is a type of public key cryptosystem that uses the modular exponent calculations, known as RSA (Rivest Shamir Adleman) cryptosystem, which is already in practical use. In this RSA cryptosystem, it has been shown that the plaintext can be obtained from the ciphertext if the prime factoring of the public key can be made (see R. Rivest, A. Shamir and L. Adleman; "A method for obtaining digital signatures and public-key cryptosystems", Comm. ACM, Vol. 21, No. 2, pp. 120-126 (1978)).

[0004] The public key cryptosystem such as RSA cryptosystem has its security based on the computational difficulty for obtaining the private key from the public key which is a publicly disclosed information, so that the security level can be increased as much when a size of the public key is increased. On the other hand, the RSA cryptosystem has been associated with a drawback that it requires a considerable amount of time for encryption/decryption because it carries out higher degree modular exponent calculations and therefore the required amount of calculations is large.

[0005] The encryption/decryption can be made faster by reducing the degree of the modular exponent calculations, for example, but that will require the reduction of the size of the public key and that in turn causes the lowering of the cryptosystem security.

[0006] In the following, the RSA cryptosystem will be described in further detail.

[0007] First, mutually different arbitrary prime numbers p and q are set as the first private key, and the first public key n is obtained as:

$$n = pq$$

while the least common multiple L of (p-1) and (q-1) is obtained as:

$$L = \mathrm{lcm}\,(p-1,\ q-1).$$

[0008] Then, an arbitrary integer e is set as the second public key, and the second private key d given by:

$$ed \equiv 1 \pmod{L}$$

is obtained using the Euclidean division algorithm.

[0009] Then, a plaintext M and its ciphertext C can be expressed as follow:

$$C \equiv M^e \pmod{n},$$

$$M \equiv C^d \pmod{n}.$$

[0010] Here, the value of the second public key e can be rather small like 13, for instance, so that the encryption processing can be made very fast, but the value of the second private key d has a size nearly equal to n so that the decryption processing will be quite slow.

[0011] On the other hand, the processing amount of the modular exponent calculations is proportional to the cube of the size of a number, so that by utilizing this property, the Chinese remainder theorem can be used in order to make the decryption processing faster.

[0012] The decryption processing using the Chinese remainder theorem proceeds as follows.

$$d_p \equiv d \pmod{p-1},$$

$$d_q \equiv d \pmod{q-1},$$

$$uq \equiv 1 \pmod{p},$$

$$M_p \equiv C^{d_p} \pmod{p},$$

$$M_q \equiv C^{d_q} \pmod{q},$$

$$M \equiv ((M_p - M_q)u \pmod{p})q + M_q,$$

where u is an inverse of q modulo p.

[0013] Here, the size of each of p, q, d_p and d_q is a half of the size of n so that the modular exponent calculations module p or q can be processed eight times faster, and as a result, the decryption processing as a whole can be made four times faster.

[0014] Also, the RSA cryptosystem can be easily cryptoanalyzed if the prime factoring of n can be made. Currently, the potentially threatening prime factoring algorithms include the number field sieve method and the elliptic curve method.

[0015] The required amount of calculations is of a quasi-exponential order of the size of n in the number field sieve method and of a quasi-exponential order of the size of a prime number in the elliptic curve method. The elliptic curve method is practically not a problem because of its high order calculations and large coefficients. On the other hand, the number field sieve method has a record for the prime factoring of the largest number realized so far, which is about 140 figures in decimal. Consequently, attacks using these methods are not threatening in practice if n is 1024 bits or so.

[0016] In addition, there are cases where a public key cryptosystem apparatus can be used as an authentication apparatus by reversing the public key and secret key calculations in general.

[0017] WO 90/02456 discloses a method whereby individual members of a group of members or entities may be provided, under the control of a trusted member, referred to as the parent, with respective individual secret keys for use i n public key cryptography, such that the matching public key can be readily derived, and group membership authenticated. The parent initially establishes a public key (e, N) where N = P.Q is the product of two primes. In response to a request from a group member, and the parent selects two further primes R, S and communicates two values dependent thereon to the requesting member, which selects two more primes T and U for use in conjunction with the received values to establish the member's secret key.

SUMMARY OF THE INVENTION

[0018] It is therefore an object of the present invention to provide a new scheme for encryption, decryption and authentication which is capable of overcoming the problems associated with the conventionally known RSA cryptosystem as described above.

[0019] More specifically, objects of the present invention are:

(1) to realize an encryption/decryption scheme which has the same security level compared with the known RSA cryptosystem on rational integer ring,
(2) to realize an encryption/decryption scheme for which the encryption/decryption processing is faster than the conventional RSA cryptosystem;
(3) to realize an encryption/decryption scheme which can also be utilized as an authentication scheme such that a single apparatus can be used for both the cipher communications and the authentication, and
(4) to realize an authentication scheme for which the authenticator generation and the verification are faster than the known authentication scheme based on the conventional RSA cryptosystem.

[0020] According to the present invention there is provided a decryption method according to the appended claim 1, an authentication method according to the appended claim 5, a decryption apparatus according to the appended claim 9, a cipher communication system according to the appended claim 10, an authentication message sender apparatus according to the appended claim 11, an authentication system according to the appended claim 12, and computer usable media according to the appended claims 13 and 14. Preferred embodiments of the invention are defined in the dependent claims.

[0021] Other features and advantages of the present invention will become apparent from the following description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022]

Fig. 1 is a block diagram of a cipher communication system according to one embodiment of the present invention.
Fig. 2 is a flow chart for an encryption processing of an encryption apparatus in the cipher communication system of Fig. 1.
Fig. 3 is a flow chart for a decryption processing of a decryption apparatus in the cipher communication system of Fig. 1.
Fig. 4 is a block diagram of an authentication system according to one embodiment of the present invention.
Fig. 5 is a flow chart for an authentication processing in the authentication system of Fig. 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0023] There may be provided an encryption method, comprising the steps of: setting N (≥ 2) prime numbers p_1, p_2, ..., p_N as a first private key, and a product $p_1^{k1}p_2^{k2} \cdots p_N^{kN}$ as a first public key n, where k1, k2, ..., kN are arbitrary positive integers; determining a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ..., p_N-1, using the first secret key; and obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

[0024] According to another aspect there is provided a decryption method for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k1}\ p_2^{k2}$ ····· p_N^{kN} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2 -1, ····· , p_N-1, the method comprising the steps of: obtaining residues $M_{p1k1}, M_{p2k2}, \cdots\cdots, M_{pNkN}$ modulo $_{p1}{}^{k1}, {}_{p2}{}^{k2}, \cdots\cdots, {}_{pN}{}^{kN}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first private key p_1, p_2, ·····, p_N ; and recovering the plaintext M by applying Chinese remainder theorem to the residues $Mp_{1k1}, M_{p2k2}, \cdots\cdots, M_{pNkN}$.

[0025] According to another aspect there may be provided an authentication method for authenticating an authentication message sent from a sender to a receiver, comprising the steps of: (a) setting at the sender side a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k1}\ p_2^{k2}$ ····· p_N^{kN} where k1, k2, ·····. kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1 -1, p_2 -1, ····· , p_N-1; (b) obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; (c) obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots, h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots, p_N^{kN}$, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1, p_2, ····· , p_N, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots, h(C)_{pNkN}$; (d) sending the encrypted authenticator h(C) and the authentication message M from the sender to the receiver; (e) obtaining at the receiver side a first authenticator $h(M)_1$ by calculating h(C)^e (mod n) from the encrypted authenticator h(C) received from the sender using the second public key e; (f) obtaining at the receiver side a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and (g) judging an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0026] According to another aspect there may be provided an encryption apparatus, comprising: an encryption/decryption key generation processing unit for setting N (≥ 2) prime numbers p_1, p_2, ····· , p_N as a first private key, and a product $p_1^{k1}p_2^{k2}$ ····· p_N^{kN} as a first public key n, where k1, k2, ·····, kN are arbitrary positive integers, and determining a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1 -1, p_2 -1, ·····, p_N-1, using the first private key; and an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

[0027] According to another aspect of the present invention there is provided a decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k1}p_2^{k2}$ ····· p_N^{kN} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1, the apparatus comprising: a calculation processing unit for obtaining residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ·····, p_N^{kN}, respectively, of the plaintext M using a prescribed loop calculation with respect to the first private key p_1, p_2, ·····, p_N ; and a decryption processing unit for recovering the plaintext M by applying Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN}.

[0028] According to another aspect there may be provided a cipher communication system, comprising: a sender apparatus having: an encryption/decryption key generation processing unit for setting N (≥ 2) prime numbers p_1, p_2, ·····, p_N as a first private key, and a product $p_1^{k1}p_2^{k2}$ ····· p_N^{kN} as a first public key n, where k1, k2, ·····, kN are arbitrary positive integers, and determining a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1, using the first private key; and an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e; and a receiver apparatus having: a calculation processing unit for obtaining residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ····· , p_N^{kN}, respectively, of the plaintext M using a prescribed loop calculation with respect to the first private key p_1, p_2, ····· , p_N ; and a decryption processing unit for recovering the plaintext M by applying Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkM}.

[0029] According to another aspect there may be provided an authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the apparatus comprising: an encryption/ decryption key generation processing unit for setting at the sender side a first private key given by N (≥ 2) prime numbers p_1, p_2 , ·····, p_N, a first public key n given by a product $P_1^{k1}{}_{p2}{}^{k2}$ ····· p_N^{kN} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1 -1, p_2 -1, ·····, p_N-1; an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ·····, $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ·····, p_N^{kN}, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first private key p_1, p_2, ····· , p_N, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ·····, $h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver.

[0030] According to another aspect of the present invention there is provided an authentication message receiver apparatus for use in authenticating an authentication message sent from a sender to a receiver, using a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product p_1^{k1} p_2^{k2} - p_N^{kn} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \cdot (\mathrm{mod}\ L)$$

where L is a least common multiple of p_1 -1 , p_2 -1, ·····, p_N-1, the apparatus comprising: an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from an encrypted authenticator h (C) received from the sender using the second public key e; an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing an authentication message M received from the sender using a hash function h; and an authenticity verification processing unit for judging an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0031] According to another aspect there may be provided an authentication system for authenticating an authentication message sent from a sender to a receiver, the system comprising: a sender apparatus having: an encryption/decryption key generation processing unit for setting at the sender side a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product p_1^{k1} p_2^{k2} ····· P_N^{kN} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \ (\mathrm{mod}\ L)$$

where L is a least common multiple of p_1 -1, p_2 -1, ·····, p_N-1; an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \ (\mathrm{mod}\ n)$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ·····, $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ·····, p_N^{kN}, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first private key p_1, p_2, ····· , p_N , and applying Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ·····, $h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver; and a receiver apparatus having: an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from the encrypted authenticator h(C) received from the sender using the second public key e; an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and an authenticity verification processing unit for judging an authenticity of the authentication message M by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0032] According to another aspect there may be provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as an encryption apparatus, the computer readable program code means includes: first computer readable program code means for causing said computer to set N (≥ 2) prime numbers p_1 , p_2, ..., p_N as a first private key, and a product p_1^{k1} p_2^{k2} ····· p_N^{kN} as a first public key n, where k1, k2, ·····, kN are arbitrary positive integers, and determining a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \cdot (\mathrm{mod}\ L)$$

where L is a least common multiple of p_1 -1, p_2 -1, ·····, P_N-1, using the first private key; and second computer readable program code means for causing said computer to obtain a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

[0033] According to another aspect of the present invention there is provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as a decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k1}\, p_2^{k2}$ ····· p_N^{kN} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1 -1, p_2 -1, ·····, p_{N-1}, the computer readable program code means includes: first computer readable program code means for causing said computer to obtain residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ·····, p_N^{kN}, respectively, of the plaintext M using a prescribed loop calculation with respect to the first private key p_1, p_2, ·····, p_N; and second computer readable program code means for causing said computer to recover the plaintext M by applying Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN}.

[0034] According to another aspect there may be provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the computer readable program code means includes: first computer readable program code means for causing said computer to set at the sender side a first private key given by N (≥ 2) prime numbers p_1, p_2 , ·····, p_N, a first public key n given by a product $p_1^{K1}\, p_2^{k2}$ ····· p_N^{kN} where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1; second computer readable program code means for causing said computer to obtain at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and third computer readable program code means for causing said computer to obtain at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ····· , $h(C)_{pNkN}$ modulo P_1^{k1}, p_2^{k2}, ·····, p_N^{kN}, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first private key p_1, p_2, ·····, p_N, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ·····, $h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver.

[0035] According to another aspect there may be provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message receiver apparatus for use in authenticating an authentication message sent from a sender to a receiver, using a first private key given by N (≥ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k1}\, p_2^{k2}$ ····· p_N^{kN} where k1,

k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1 - 1$, $p_2 - 1$, ·····, $p_N - 1$, the computer readable program code means includes: first computer readable program code means for causing said computer to obtain a first authenticator $h(M)_1$ by calculating $h(C)^e \pmod{n}$ from an encrypted authenticator h(C) received from the sender using the second public key e; second computer readable program code means for causing said computer to obtain a second authenticator $h(M)_2$ by hashing an authentication message M received from the sender using a hash function h; and third computer readable program code means for causing said computer to judge an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0036] Referring now to Fig. 1 to Fig. 4, one embodiment of the scheme for encryption, decryption and authentication according to the present invention will be described in detail.

[0037] Note that the encryption/decryption scheme of the present invention is realizable using $n = p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ in general, as will be described below, but the more practical exemplary case of using $n = p_1^{k1} p_2$ will be described first. In the following, an expression "$p^k q$" corresponds to a special case of the general expression $p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ (where $p_1, p_2, \cdots\cdots, p_N$ are N (≥ 2) prime numbers) with N = 2, $p_1 = p$, $p_2 = q$, k1 = k and k2 = 1.

[0038] Fig. 1 shows an overall configuration of a cipher communication system according to one embodiment of the present invention.

[0039] The cipher communication system of Fig. 1 generally comprises an encryption apparatus 10 and a decryption apparatus 19 which are connected through a communication path 14. The encryption apparatus 10 has an encryption processing unit 13 for obtaining a ciphertext C from a plaintext M given as its input, and transmitting the obtained ciphertext C to the decryption apparatus 19 through the communication path 14. The decryption apparatus 19 has a decryption processing unit 15 for recovering the plaintext M from the ciphertext C transmitted by the encryption processing unit 13, and outputting the obtained plaintext M as its output. This decryption processing unit 15 includes a loop calculation processing unit 17.

[0040] In addition, the encryption apparatus 10 also has an encryption/decryption key generation processing unit 11 connected with both the encryption processing unit 13 and the decryption processing unit 15, for supplying the first public key n and the second public key e to the encryption processing unit 13 while supplying the firstprivatekey p. q, the second private key d, an arbitrary positive integer k, the first public key n and the second public key e to the decryption processing unit 15.

[0041] Next, the operation of the encryption apparatus 10 will be described in detail with reference to Fig. 2.

[0042] First, the encryption/decryption keys are generated at the encryption/decryption key generation processing unit 11 as follows (step S101).

[0043] Here, the first private key is to be given by two rational prime numbers p and q, and the first public key is to be given by their product, i.e., $n = p^k q$. Also, using the function lcm for obtaining the least common multiple, L given by:

$$L = \mathrm{lcm}\,(p-1,\ q-1)$$

is obtained from the first private key p and q.

[0044] Next, e and d that satisfies:

$$ed \equiv 1 \pmod{L}$$

are obtained. Then, the residues d_p and d_q of the obtained d modulo (p-1) and (q-1) respectively are obtained as:

$$d_p := d \pmod{p-1},$$

$$d_q := d \pmod{q-1},$$

where a symbol ":=" denotes the operation to calculate the right hand side and substitute it into the left hand side, and a set of three numbers d, dp and dq is set as the second private key, while e is set as the second public key. In this way, the first public key n, the second public key e, the first private key p, q, and the second private key d, d_p and d_q are set up.

[0045] Then, the ciphertext C is obtained at the encryption processing unit 13 as follows (step S102).

[0046] The encryption processing unit 13 encrypts the plaintext M by using the first public key n and the second public key e, according to the formula:

$$C \equiv M^e \pmod{n}$$

and transmits the obtained ciphertext C to the receiving side.

[0047] Next, the operation of the decryption apparatus 19 will be described in detail with reference to Fig. 3.

[0048] The decryption processing unit 15 obtains the plaintext M as an output from the ciphertext C entered from the encryption processing unit 13 through the communication path, the first private key p, q, the second private key d, the second public key e and the arbitrary positive integer k which are entered from the encryption/decryption key generation processing unit 11, by carrying out the following substitution calculation processing, where a symbol ":=" denotes the operation to calculate the right hand side and substitute it into the left hand side.

[0049] (Step S201) The values d_p and d_q of the second secret key d modulo p-1 and q-1 respectively are obtained as follows.

$$d_p := d \pmod{p-1},$$

$$d_q := d \pmod{q-1}.$$

Note that there is no need to calculate these d (mod p-1) and d (mod q-1) at every occasion of the encryption/decryption and it suffices to produce them once in advance as the private key. In such a case, d will be necessary only at the intermediate stage for producing these d (mod p-1) and d (mod q-1).

[0050] (Step S202) The residues K_{00}, M_q of the plaintext M modulo p and q respectively are obtained from the ciphertext C as follows.

$$K_0 := C^{d_p} \pmod{p},$$

$$M_0 := C^{d_q} \pmod{q}.$$

[0051] (Step S203) The residue M_{pk} of the plaintext M modulo p^k is obtained by carrying out the following loop calculation according to the fast decryption algorithm disclosed in T. Takagi, "Fast RSA-type cryptosystem using n-adic expansion", Advances in Cryptology - CRYPTO'97, LNCS 1294, pp. 372-384 and in U.S. Patent Application Serial No. 08/907,852 of the present inventors, at the loop calculation processing unit 17.

$$A_0 := K_0 ;$$

FOR i = 1 to (k-1) do
begin

$$F_i := (A_{i-1}^e) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i / p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p};$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

end

$$M_{pk} := A_{k-1}.$$

[0052] (Step S204) The residue of the plaintext M with respect to a composite number n is obtained by applying the Chinese remainder theorem to the residues M_{pk} and M_q, so as to complete the decryption.

[0053] More specifically, the Chinese remainder theorem can be applied by the following calculation.

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((M_{pk} - M_q) q_1) \pmod{p^k};$$

$$M := (M_q + q v_1).$$

[0054] Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((M_q - M_{pk}) p_1) \pmod{q};$$

$$M := (M_{pk} + p^k v_1).$$

[0055] Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k};$$

$$M := (q_1 q M_{p\,k} + p_1 p^k M_q) \pmod{p^k q}.$$

[0056] Next, the functions of the respective processing units in the cipher communication system of Fig. 1 will be described along their processing procedure.

[0057] First, as the first stage, at the encryption/decryption key generation processing unit 11, two prime numbers p and q to be the first private key are generated, and the product $n = p^k q$ of these two prime numbers p and q is obtained as the first public key. Here, k is an arbitrary integer to be selected by accounting for the security level and the processing speed. Also, as can be seen from the formula $n = p^k q$ for the first public key n, the sizes of p and q can be made smaller when k is larger for a constant size (the number of digits, for example) of n, and the prime factoring becomes as much easier (that is, it becomes easier to learn the values of p and q) so that the security level of this cryptosystem becomes lower.

[0058] Next, the least common multiple L is calculated from these two prime numbers p and q, and the second pubic key e and the second private key d are generated according to $ed \equiv 1 \pmod{L}$. This calculation of the least common multiple L can be done by first obtaining the greatest common divisor using the extended Euclidean division algorithm and then multiplying the remaining factors to obtain the least common multiple.

[0059] Note that the pair of e and d at this point is uniquely determined from $ed \equiv 1 \pmod{L}$. Although it can be any pair that satisfies this condition in principle, usually the second public key e is set to be a smaller value in order to make the encryption faster. For this reason, the second private key d becomes a considerably large number so that the decryption processing becomes slow when the conventional scheme is adopted. Note that the second public key e and the second private key d are in relationship of inverse numbers modulo L, so that the second private key d can be obtained if the second public key e and the least common multiple L are known.

[0060] Next, as the second stage, at the encryption processing unit 13, the encryption is carried out according to the formula:

$$C \equiv M^e \pmod{n}$$

using the second public key e of the receiving side, and the ciphertext C is transmitted to the receiving side.

[0061] Then, as the third stage, at the decryption processing unit 15, M_{pk} M (mod p^k) and $M_q \equiv C^{dq} \pmod{q}$ are obtained using the aforementioned fast decryption algorithm, and the Chinese remainder theorem is applied to these two numbers. According to the Chinese remainder theorem, when the residues of an unknown number for plural moduli are known, the unknown number (solution) modulo a product of these plural moduli can be obtained uniquely so that M can be recovered.

[0062] Now, concrete examples of the encryption according to this embodiment will be described.

[0063] First, the exemplary case of k = 2 can be summarized as follows.

Public key e = 5
Public key n = 40270132689707
Private key d = 234982541
Private key p = 34273
Private key q = 34283
Plaintext M = 1234567890
Ciphertext C = 10229049760163
$A_\emptyset = K_\emptyset = 20157$
$M_\emptyset = 2777$
$K_1 = 1748$
$M_p = A_\emptyset + pK_1 = 59929361$
Plaintext M = 1234567890

[0064] In this case, the value of each one of the first private key p and q is about $n^{1/(k+1)}$, and the least common multiple L is about $n^{2/(k+2)}$ which is smaller than the RSA cryptosystem so that it can contribute to the realization of the faster encryption/decryption.

[0065] More specifically, the calculation time for C^d mod n is $0((\log n)^2(\log d))$ while the calculation time for C^d mod p and C^d mod q is $0(1/3 \log n)^2(2/3 \log n)$. Thus the overall processing time is 0.148 times that of the RSA cryptosystem, and it is a little over three times faster than the Quisquater-Couvreur scheme that utilizes the Chinese remainder theorem

(which has the calculation time of $O(1/2 \log n)^2(1 \log n)$).

[0066] Next, the exemplary case of k = 3 can be summarized as follows.

Public key e = 5
Public key n = 627252701350243
Private key d = 7515005
Private key p = 5003
Private key q = 5009
Plaintext M = 123456789012345
Ciphertext C = 287551735059915
$A_{\emptyset} = K_{\emptyset p} = 1732$
$M_q = 3412$
$K_{1p} = 4821$
$A_1 = 24121195$
$K_{2p} = 4395$
$M_p 2 = A_2 = A_1 + p^2K_2 = 110031010750$
Plaintext M = 123456789012345

[0067] It should be apparent that the encryption/decryption scheme described above is also applicable to the case of using three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ as the first private key and a product $p^k q^\ell r^m$ where k = k1, ℓ = k2 and m = k3 as the first public key n.

[0068] In this case, the decryption can be realized by first obtaining $K_{\emptyset}{}^p$, $K_{\emptyset}{}^q$ and $K_{\emptyset}{}^r$ modulo p, q and r, respectively, by integer modular exponent calculations of:

$$K_{\emptyset}{}^p := C^{d\,p} \pmod{p};$$

$$K_{\emptyset}{}^q := C^{d\,q} \pmod{q};$$

$$K_{\emptyset}{}^r := C^{d\,r} \pmod{r};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1};$$

$$dr := d \pmod{r-1};$$

next obtaining the residues M_{pk}, $M_{q\ell}$ and M_{rm} modulo p^k, q^ℓ and r^m, respectively, by applying the loop calculation to $K_{\emptyset}{}^p$, $K_{\emptyset}{}^q$ and $K_{\emptyset}{}^r$, respectively, and then applying the Chinese remainder theorem to the residues M_{pk}, $M_{q\ell}$ and M_{rm}.

[0069] It should also be apparent that the encryption/decryption scheme described above can be generalized to the case of using N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots, p_N$ as a first private key, and a product $p_1{}^{k1}\, p_2{}^{k2} \cdots\cdots p_N{}^{kN}$ as a first

public key n, where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1 - 1$, $p_2 - 1$, ·····, $P_N - 1$.

[0070] In this general case, a ciphertext C can be obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e defined above.

[0071] Also in this case, the decryption can be realized by first obtaining residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ····· , p_N^{kN}, respectively, of the plaintext M using the loop calculation of the aforementioned fast decryption algorithm with respect to the first private key p_1, p_2, ·····, p_N, and then applying the Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ·····, M_{pNkN}.

[0072] Next, Fig. 4 shows an overall configuration of an authentication system according to one embodiment of the present invention.

[0073] The authentication system of Fig. 4 generally comprises a sender apparatus 20 and a receiver apparatus 33 which are connected through a communication path 26. The sender apparatus 20 has an authentication message hashing processing unit 23 for outputting an authenticator h(M) by applying a hashing processing on an input authentication message (plaintext) M, and an authenticator encryption processing unit 25 for encrypting the authenticator h(M) outputted from the authentication message hashing processing unit 23 and transmitting the obtained encrypted authenticator h (C) through a communication path 26.

[0074] The receiver apparatus 33 has an authenticator decryption processing unit 27 for obtaining a first authenticator $h(M)_1$ from the encrypted authenticator h(C) and an authentication message hashing processing unit 29 for obtaining a second authenticator $h(M)_2$ from the authentication message M, both of which are connected to the authentication encryption processing unit 25 through the communication path 26, and an authenticity verification processing unit 31 for verifying an authenticity of the authentication message M, which is connected with the authenticator decryption processing unit 27 and the authentication message hashing processing unit 29.

[0075] In addition, the sender apparatus 20 also has an authentication encryption/decryption key generation processing unit 21 for outputting authentication encryption/decryption keys to the authenticator encryption processing unit 25 and the authenticator decryption processing unit 27 respectively.

[0076] This authentication system of Fig. 4 realizes the authentication scheme in which a person who wishes to have the own authentication message authenticated will send to the receiving side an authenticator generated by encrypting the authentication message by using the own private key.

[0077] Now, the operations of the respective processing units in the authentication system of Fig. 4 will be described along their processing procedure with reference to Fig. 5.

[0078] First, as the first stage (step S301), at the authentication encryption/decryption key generation processing unit 21, two prime numbers p and q to be the first private key are generated, and the product $n = p^k q$ of these two prime numbers p and q is obtained as the first public key. Here, k is an arbitrary integer to be selected by accounting for the security level and the processing speed. Also, as can be seen from the formula $n = p^k q$ for the first public key n, the sizes of p and q can be made smaller when k is larger for a constant size (the number of digits, for example) of n, and the prime factoring becomes as much easier (that is, it becomes easier to learn the values of p and q) so that the security level of this cryptosystem becomes lower. Then, the least common multiple L is calculated from these two prime numbers p and q, and the second pubic key e and the second private key d are generated according to $ed \equiv 1 \pmod{L}$.

[0079] Next, as the second stage (step S302), at the authentication message hashing processing unit 23, the plaintext authentication message M is hashed by using the hash function h to obtain the authenticator h(M), where it is assumed that $0 \leq h(M) < n$. Here, the hash function is used in order to shorten the message length. For example, the hashing processing extracts several characters from the top of the message. Also, a certain level of the scrambling function is to be provided. Note that the same hash function is to be used at the sending side and the receiving side.

[0080] Next, as the third stage (step S303), at the authenticator encryption processing unit 25, the encrypted authenticator h(C) is calculated by the technique of the aforementioned fast decryption algorithm, using the first public key n and the second private key d of the sending side. Note that, in the authentication, the decryption processing and the encryption processing become completely reversed from the case of the encryption/decryption scheme described above,

so that the calculation of the encrypted authenticator h(C) can be processed quickly by using the Chinese remainder theorem.

[0081] After this calculation processing, the set of the encrypted authenticator h(C) and the authentication message M is transmitted to the receiving side through the communication path.

[0082] Next, as the fourth stage (step S304), at the authenticator decryption processing unit 27, the receiving side decrypts the encrypted authenticator h(C) by calculating:

$$h(M)_1 \equiv h(C)^e \pmod{n}$$

using the second public key e of the sending side, so as to obtain the first authenticator $h(M)_1$.

[0083] Next, as the fifth stage (step S305), at the authentication message hashing processing unit 29, the receiving side hashes the authentication message M by using the hash function h so as to obtain the second authenticator $h(M)_2$.

[0084] Then, as the sixth stage (step S306), at the authenticity verification processing unit 31, the authenticity of the authentication message is judged according to whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide with each other or not, and an output indicating either coincide (Yes) or not coincide (No) is outputted.

[0085] More specifically, the authentication scheme according to the present invention can be realized as follows.

[0086] In the most general case, the sender side sets a first private key given by N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots, p_N-1$.

[0087] Then, the sender side obtains an authenticator h(M) by hashing the authentication message M using a hash function h, while obtaining an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots, h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots, p_N^{kN}$, respectively, of the encrypted authenticator h(C) using the loop calculation of the aforementioned fast decryption algorithm with respect to the first private key $p_1, p_2, \cdots\cdots, p_N$, and applying the Chinese remainder theorem to the residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots, h(C)_{pNkN}$.

[0088] Then, the encrypted authenticator h(C) and the authentication message M are sent from the sender to the receiver.

[0089] Next, the receiver side obtains a first authenticator $h(M)_1$ by calculating $h(C)^e \pmod{n}$ from the encrypted authenticator h(C) received from the sender using the second public key e, while obtaining a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h.

[0090] Then, an authenticity of the authentication message M is judged at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0091] It should be apparent from the above that, in the specific case where the encrypted authenticator h(C) is obtained using the first private key given by three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ and the first public key n given by a product $p^k q^\ell r^m$ where k = k1, ℓ = k2 and m = k3, the sender obtains the encrypted authenticator h(C) by first obtaining $h(K)_\emptyset{}^p$, $h(K)_\emptyset{}^q$ and $h(K)_\emptyset{}^r$ modulo p, q and r, respectively, by integer modular exponent calculations of:

$$h(K)_\emptyset{}^p := h(M)^{d_p} \pmod{p};$$

$$h(K)_\emptyset{}^q := h(M)^{d_q} \pmod{q};$$

$$h(K)_{\emptyset}{}^{r} := h(M)^{dr} \pmod{r};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1};$$

$$dr := d \pmod{r-1};$$

next obtaining the residues $h(C)_{pk}$, $h(C)_{q\ell}$ and $h(C)_{rm}$ modulo p^k, q^ℓ and r^m, respectively, by applying the loop calculation to $h(K)_{\emptyset}{}^{p}$, $h(K)_{\emptyset}{}^{q}$ and $h(K)_{\emptyset}{}^{r}$, respectively, and then applying the Chinese remainder theorem to the residues $h(C)_{pk}$, $h(C)_{q\ell}$ and $h(C)_{rm}$.

[0092] It should also be apparent from the above that, in the specific case where the encrypted authenticator h(C) is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by a product $p^k q$ where $k = k1$, the sender obtains the encrypted authenticator h(C) by first obtaining a residue $h(K)_{\emptyset}$ modulo p and a residue $h(C)_q$ modulo q of the encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_{\emptyset} := h(M)^{dp} \pmod{p};$$

$$h(C)_{q} := h(M)^{dq} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1};$$

next obtaining a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the loop calculation to $h(K)_{\emptyset}$, and then applying the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$.

[0093] In this case, the loop calculation can be carried out as follows.

$$h(A)_{\emptyset} := h(K)_{\emptyset};$$

FOR i = 1 to (k-1) do
begin

$$h(F)_i := (h(A)_{i-1}{}^{e}) \pmod{p^{i+1}};$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := h(E)_i / p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

end

$$h(C)_{pk} := h(A)_{k-1}.$$

[0094] Also in this case, the Chinese remainder theorem can be applied by the following calculation.

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((h(C)_{pk} - h(C)_q) q_1) \pmod{p^k};$$

$$h(C) := (h(C)_q + q v_1).$$

Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((h(C)_q - h(C)_{pk}) p_1) \pmod{q};$$

$$h(C) := (h(C)_{pk} + p^k v_1).$$

Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k};$$

$$h(C) := (q_1 q h(C)_{pk} + p_1 p^k h(C)_q) \pmod{p^k q}.$$

[0095] Note that, in the above described embodiment, each of the prime numbers has a size of about $n^{1/(k+1)}$ which

is sufficient to prevent the number field sieve method and the elliptic curve method that are the fastest prime factoring algorithms currently known. Also, the second public key e can be set small so that the second private key d has about the same size as the least common multiple L. Here, the least common multiple L has a size of $n^{2/(k+1)}$ which is smaller than that of the RSA cryptosystem so that it can contribute to the realization of the faster encryption/decryption.

[0096] Also, in the above described embodiment, the case of k = 3 uses the composite number $n = p^3q$ as the modulus, so that the size of each of p and q becomes 1/4 of the size of n. The decryption processing modulo p^3 requires about the same amount of calculations as the processing modulo p, so that the processing modulo p^3 and the processing modulo q can be made 64 times faster. Thus the overall processing can be made 32 times faster, which is considerably faster even in comparison with the conventional Quisquater-Couvreur scheme that can realize four times faster decryption processing than the original RSA cryptosystem.

[0097] As described, the cryptosystem according to the present invention uses N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots, p_N$ as the first private key and their product $p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ as the first public key n, so that it has the same security level as the conventionally known RSA cryptosystem on rational integer ring, while it is capable of realizing the faster encryption and decryption processing. In addition, it can be utilized for the authentication as well, and it is also capable of realizing the faster authenticator generation and authenticity verification.

[0098] Moreover, the cryptosystem according to the present invention uses the second public key e as an encryption key and the second private key d as a decryption key which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots, p_N-1$, so that the size of the decryption key d can be made about the same as the size of L.

[0099] In contrast, in the case of the RSA cryptosystem for example, if $p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ is to be used as the first public key n where $p_1, p_2, \cdots\cdots, p_N$ are N (≥ 2) prime numbers, it is required to generate the encryption key e and the decryption key d which satisfy:

$$ed \equiv 1 \pmod{\phi(n)}$$

where

$$\phi(n) = n(1-1/p_1)(1-1/p_2)\cdots(1-1/p_N)$$

is the Euler function, so that the size of the decryption key d becomes the same as the size of $\phi(n)$ which is considerably larger than the size of L.

[0100] It is to be noted that the above described embodiment according to the present invention may be conveniently implemented in forms of software programs for realizing the operations of the cipher communication system of Fig. 1 or the authentication system of Fig. 4, as will be apparent to those skilled in the computer art. Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.

[0101] In particular, each of the encryption apparatus and the decryption apparatus of Fig. 1 and the sender apparatus and the receiver apparatus of Fig. 4 as described above can be conveniently implemented in a form of a software package.

[0102] Such a software package can be provided in a form of a computer program product which employs a storage medium including stored computer code which is used to program a computer to perform the disclosed function and process of the present invention. The storage medium may include, but is not limited to, any type of conventional floppy disks, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or any other suitable media for storing electronic instructions.

[0103] It is also to be noted that, besides those already mentioned above, many modifications and variations of the above embodiments may be made without departing from the novel and advantageous features of the present invention. Accordingly, all such modifications and variations are intended to be included within the scope of the appended claims.

Claims

1. A decryption method for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first private key given by N ≥ 2 prime numbers p_1, p_2, ..., p_N, a first public key n given by a product p_1^{k1}, p_2^{k2}, ..., p_N^{kN} where k1, k2, ..., kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is the least common multiple of p_1-1, p_2-1, ..., p_N-1, the method comprising the steps of:

obtaining residues M_{p1k1}, M_{p2k2}, ..., M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN}, respectively, of the plaintext M using a loop calculation with respect to the first private key p_1, p_2, ..., p_N : and
recovering the plaintext M by applying the Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ..., M_{pNkN};

CHARACTERIZED IN THAT

the ciphertext C is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product p^kq where k = k1 ;
the obtaining step obtains a residue $K_ø$ modulo p and a residue M_q modulo q of the plaintext M, by integer modular exponent calculations of:

$$K_ø := C^{d_p} \pmod{p};$$

and

$$M_q := C^{d_q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and obtains a residue M_{pk} modulo p^k of the plaintext M by applying the loop calculations to $K_ø$; and
the recovering steps applies the Chinese remainder theorem to the residues M_{pk} and M_q; and
the loop calculation is carried out by:

(a) setting $A_Ø := K_Ø$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$F_i := (A_{i-1}^e) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p};$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

and
(c) setting $M_{pk} := A_{k-1}$.

2. The method of claim 1, wherein the recovering step recovers the plaintext M by calculating:

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((M_{p\,k} - M_q)\ q_1) \pmod{p^k};$$

and

$$M := (M_q + qv_1).$$

3. The method of claim 1, wherein the recovering step recovers the plaintext M by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((M_q - M_{p\,k})\ p_1) \pmod{q};$$

and

$$M := (M_{p\,k} + p^k\ v_1).$$

4. The method of claim 1, wherein the recovering step recovers the plaintext M by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k};$$

and

$$M := (q_1 \, qM_{p\,k} + p_1 \, p^k \, M_q) \pmod{p^k q} .$$

5. An authentication method for authenticating an authentication message sent from a sender to a receiver, comprising the steps of:

(a) setting at the sender side a first private key given by $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} ... p_N^{kN}$ where k1, k2, ... kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_N-1$;
(b) obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h;
(c) obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, respectively, of the encrypted authenticator h(C) using a loop calculation with respect to the first private key $p_1, p_2, ..., p_N$; and applying the Chinese remainder theorem to the residues $h(C)_{p1k1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$;
(d) sending the encrypted authenticator h (C) and the authentication message M from the sender to the receiver;
(e) obtaining at the receiver side a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from the encrypted authenticator h(C) received from the sender using the second public key e;
(f) obtaining at the receiver side a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and
(g) judging the authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not;

CHARACTERIZED IN THAT

the encrypted authenticator h(C) is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product $p^k q$ where $k = k1$;
the step (c) obtains a residue $h(K)_p$ modulo p and a residue $h(C)_q$ modulo q of encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_p := h(M)^{d\,p} \pmod{p};$$

and

$$h(C)_q := h(M)^{d\,q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and obtains a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the loop calculation to $h(K)_{\varnothing}$, and applies the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$; and
the loop calculation is carried out by:

(a) setting $h(A)_{\varnothing} := h(K)_{\varnothing}$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$h(F)_i := (h(A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

and
(c) setting $h(C)_{pk} := h(A)_{k-1}$.

6. The method of claim 5, wherein the step (c) applies the Chinese remainder theorem by calculating:

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((h(C)_{p\,k} - h(C)_q)\ q_1) \pmod{p^k};$$

and

$$h(C) := (h(C)_q + qv_1).$$

7. The method of claim 5, wherein the step (c) applies the Chinese remainder theorem by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((h(C)_q - h(C)_{p\,k})\ p_1) \pmod q;$$

and

$$h(C) := (h(C)_{p\,k} + p^k\ v_1).$$

8. The method of claim 5, wherein the step (c) applies the Chinese remainder theorem by calculating:

$$p_1 := (p^k)^{-1} \pmod q;$$

$$q_1 := q^{-1} \pmod{p^k};$$

and

$$h(C) := (q_1\ qh(C)_{p\,k} + p_1\ p^k\ h(C)q) \pmod{p^kq}.$$

9. A decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod n$$

using a first private key given by $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$, a first public key n given by a product $p_1^{k1}\ p_2^{k2} ... p_N^{kN}$ where k1, k2, ..., kN are arbitrary positive integers, a second public key e and a second private key key d which satisfy:

$$ed \equiv 1 \pmod L$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_N-1$, the apparatus comprising:

a calculation processing unit for obtaining residues $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$ module $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, respectively, of the plaintext M using a loop calculation with respect to the first private key $p_1, p_2, ..., p_N$; and
a decryption processing unit for recovering the plaintext M by applying the Chinese remainder theorem to the residues $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$;

CHARACTERIZED IN THAT

the ciphertext C is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product p^kq where $k = k1$;
the calculation processing unit is adapted to obtain a residue $K_\varnothing$ modulo p and a residue M_q modulo q of the plaintext M, by integer modular exponent calculations of:

$$K_\varnothing := C^{d\,p} \pmod p;$$

and

$$M_q := C^{d_q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and is adapted to obtain a residue M_{pk} modulo p^k of the plaintext M by applying the loop calculation to $K_ø$; and the recovering decryption processing unit is adapted to apply the Chinese remainder theorem to the residues M_{pk} and M_q; and
the loop calculation is carried out by:

(a) setting $A_ø := K_ø$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$F_i := (A_{i-1}^e) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p};$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

and
(c) setting $M_{pk} := A_{k-1}$.

10. A cipher communication system, comprising:

a sender apparatus having:

an encryption/decryption key generation processing unit for setting $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$ as a first private key, and a product $p_1^{k1} p_2^{k2} \cdots p_N^{kN}$ as a first public key n, where k1, k2, ..., kN are arbitrary positive integers, and determining a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_N-1$, using the first private key; and
an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e; and

a receiver apparatus having:

a calculation processing unit for obtaining residues M_{p1k1}, M_{p2k2}, ..., M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN}, respectively, of the plaintext M using a loop calculation with respect to the first private key p_1, p_2, ..., p_N; and a decryption processing unit for recovering the plaintext M by applying the Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ..., M_{pNkN};

CHARACTERIZED IN THAT

the ciphertext C is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product $p^k q$ where k = k1;
the calculation processing unit is adapted to obtain a residue $K_\emptyset$ modulo p and a residue M_q modulo q of the plaintext M, by integer modular exponent calculations of:

$$K_\emptyset := C^{d\,p} \pmod{p};$$

and

$$M_q := C^{d\,q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and is adapted to obtain a residue M_{pk} modulo p^k of the plaintext M by applying the loop calculation to $K_\emptyset$; and the decryption processing unit is adapted to apply the Chinese remainder theorem to the residues M_{pk} and M_q; and
the loop calculation is carried out by:

(a) setting $A_\emptyset := K_\emptyset$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$F_i := (A_{i-1}^e) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod p;$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

and
(c) setting $M_{pk} := A_{k-1}$.

11. An authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the apparatus comprising:

an encryption/decryption key generation processing unit for setting at the sender side a first private key given by $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$ a first public key n given by a product $p_1^{k1} p_2^{k2} ... p_N^{kN}$ where k1, k2, ..., kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod L$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_N-1$;
an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and
an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod n$$

by obtaining residues $h(C)_{p1k1}, h(C)_{p2k2}..., h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, respectively, of the encrypted authenticator h(C) using a loop calculation with respect to the first private key $p_1, p_2, ..., p_N$, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$ and then sending the encrypted authenticator h(C) and the authentication message M to the receiver;

CHARACTERIZED IN THAT

the encrypted authenticator h(C) is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product $p^k q$ where k= k1;
the authentication encryption processing unit is adapted to obtain a residue $h(K)_ø$ modulo p and a residue $h(C)_q$ modulo q of the encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_ø := h(M)^{d_p} \pmod p;$$

and

$$h(C)_q := h(M)^{d_q} \pmod q;$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and is adapted to obtain a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the loop calculation to $h(K)_{\phi}$, and to apply the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$; and the loop calculation is carried out by:

(a) setting $h(A)_{\phi} := h(K)_{\phi}$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$h(F)_i := (h(A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

and
(c) setting $h(C)_{pk} := h(A)_{k-1}$.

12. An authentication system for authentication of an authentication message sent from a sender to a receiver, the system comprising:

a sender apparatus having:

an encryption/decryption key generation processing unit for setting at the sender side a first private key given by $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$ a first public key n given by a product $p_1{}^{k1} p_2{}^{k2} ... p_N{}^{kN}$ where k1, k2, ..., kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_N-1$;
an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and
an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h (C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN}, respectively, of the encrypted authenticator h(C) using a loop calculation with respect to the first private key p_1, p_2, ..., p_N, and applying the Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)p_{2k2}$, ..., $h(C)_{pNkN}$ and then sending the encrypted authenticator h(C) and the authentication message M to the receiver; and

a receiver apparatus having:

an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from the encrypted authenticator h(C) received from the sender using the second public key e;
an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and
an authenticity verification processing unit for judging an authenticity of the authentication message M by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not;

CHARACTERIZED IN THAT

the encrypted authenticator h(C) is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product $p^k q$ where $k = k1$;
the authentication encryption processing unit is adapted to obtain a residue $h(K)_{\varnothing}$ modulo p and a residue $h(C)_q$ modulo q of the encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_{\varnothing} := h(M)^{d_p} \pmod{p};$$

and

$$h(C)_q := h(M)^{d_q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and is adapted to obtain a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the loop calculation to $h(K)_{\varnothing}$, and to apply the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$; and
the loop calculation is carried out by:

(a) setting $h(A)_{\varnothing} := h(K)_{\varnothing}$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$h(F)_i := (h(A)_{i-1}^e) \pmod{p^{i+1}};$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

and
(c) setting $h(C)_{pk} := h(A)_{k-1}$.

13. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as a decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first private key given by $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$ a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots p_N^{kN}$, where k1, k2, ..., kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_N-1$, the computer readable program code means includes:

first computer readable program code means for causing said computer to obtain residues $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$ modulo $P_1^{k1}, p_2^{k2}, ..., P_N^{kN}$, respectively, of the plaintext M using a loop calculation with respect to the first private key $p_1, p_2, ..., p_N$; and
second computer readable program code means for causing said computer to recover the plaintext M by applying the Chinese remainder theorem to the residues $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$;

CHARACTERIZED IN THAT

the ciphertext C is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product $p^k q$ where $k = k1$:
the first computer readable program code means obtains a residue $K_ø$ modulo p and a residue M_q modulo q of the plaintext M, by integer modular exponent calculations of:

$$K_ø := C^{d_p} \pmod{p};$$

and

$$M_q := C^{d_q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and obtains a residue M_{pk} modulo p^k of the plaintext M by applying the loop calculations to $K_{\emptyset}$: and
the second computer readable program code means applies the Chinese remainder theorem to the residues M_{pk} and M_q; and
the loop calculation is carried out by:

(a) setting $A_{\emptyset} := K_{\emptyset}$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$F_i := (A_{i-1}^{e}) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p};$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

and
(c) setting $M_{pk} := A_{k-1}$.

14. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the computer readable program code means includes:

first computer readable program code means for causing said computer to set at the sender side a first private key given by $N \geq 2$ prime numbers $p_1, p_2, ..., p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots p_N^{kN}$, where k1, k2, ..., kN are arbitrary positive integers, a second public key e and a second private key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is the least common multiple of $p_1-1, p_2-1, ..., p_{N-1}$;
second computer readable program code means for causing said computer to obtain at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and
third computer readable program code means for causing said computer to obtain at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^{e} \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN}, respectively, of the encrypted authenticator h(C) using a loop calculation with respect to the first private key p_1, p_2, ..., p_N, and applying the Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver:

CHARACTERIZED IN THAT

the encrypted authenticator h(C) is obtained using the first private key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by the product $p^k q$ where $k = k1$;
the third computer readable program code means obtains a residue $h(K)_ø$ modulo p and a residue $h(C)_q$ modulo q of encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_ø := h(M)^{d_p} \pmod{p};$$

and

$$h(C)_q := h(M)^{d_q} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

and

$$dq := d \pmod{q-1};$$

and obtains a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the loop calculation to $h(K)_ø$, and applies the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$; and
the loop calculation is carried out by:

(a) setting $h(A)_ø := h(K)_ø$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$h(F)_i := (h(A)_{i-1}^e) \pmod{p^{i+1}};$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := (h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

and
(c) setting $h(C)_{pk} := h(A)_{k-1}$.

Patentansprüche

1. Entschlüsselungsverfahren zum Entschlüsseln eines Chiffre-Textes C, der aus einem Klartext M erhalten wird, gemäß:

$$C = M^e \pmod{n}$$

unter Verwendung eines ersten privaten Schlüssels, der durch $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$ gegeben ist, eines ersten öffentlichen Schlüssels n, der durch ein Produkt $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$ gegeben ist, wobei k1, k2, ..., kN beliebige positive Ganzzahlen sind, eines zweiten öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod{L}$$

wobei L das kleinste gemeinsame Vielfache von $p_1-1, p_2-1, ..., p_N-1$ ist, wobei das Verfahren die Schritte umfasst:

Erhalten von Rediduen $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_n^{kN}$ jeweils des Klartextes M unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels $p_1, p_2, ..., p_N$; und
Wiedergewinnen des Klartextes M durch ein Anwenden des chinesischen Restsatzes auf die Residuen $M_{pk1}, M_{p2k2}, ..., M_{pNkN}$;

dadurch gekennzeichnet, dass

der Chiffre-Text C unter Verwendung des ersten privaten Schlüssels, der durch zwei Primzahlen $p_1 = p$ und $p_2 = q$ gegeben ist, und des ersten öffentlichen Schlüssels n, der durch das Produkt p^kq gegeben ist, erhalten wird, wobei $k = k1$;
der Erhaltungsschritt ein Residuum $K_\varnothing$ modulo p und ein Residuum M_q modulo q des Klartextes M durch ganzzahlige modulare Exponentenberechnungen von:

$$k_\varnothing := C^{d\ p} \pmod{p};$$

und

$$M_q := C^{d\ q} \pmod{q};$$

wobei:

$$dp := d \pmod{p-1};$$

und

$$dq := d \pmod{q-1};$$

erhält, und ein Residuum M_{pk} modulo p^k des Klartextes M beim Anwenden der Schleifenberechnungen aus $K_\varnothing$ erhält; und
die Wiedergewinnungsschritte den chinesischen Restsatz auf die Residuen M_{pk} und M_q anwenden; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $A_{\emptyset} := K_{\emptyset}$;
(b) für i = 1 bis (k-1), wiederholtes Berechnen:

$$F_i := (A_{i-1}^{e}) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p};$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

und
(c) Setzen von $M_{pk} := A_{k-1}$.

2. Verfahren nach Anspruch 1, wobei der Wiedergewinnungsschritt den Klartext M durch ein Berechnen wiedergewinnt:

$$q_1 := q^{-1} \pmod{p^k};$$

$$v1 := ((M_{p\ k} - M_q)\ q_1) \pmod{p^k};$$

und

$$M := (M_q + qv_1).$$

3. Verfahren nach Anspruch 1, wobei der Wiedergewinnungsschritt den Klartext M durch ein Berechnen wiedergewinnt:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v1 := ((M_q - M_{p\ k})\ p_1) \pmod{q};$$

und

$$M := (M_{p\ k} + p^k\ v_1).$$

4. Verfahren nach Anspruch 1, wobei der Wiedergewinnungsschritt den Klartext M durch ein Berechnen wiedergewinnt:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k};$$

und

$$M := (q_1 \, q M_{p\,k} + p_1 \, p^k \, M_q) \pmod{p^k q}.$$

5. Authentifizierungsverfahren zum Authentifizieren einer Authentifizierungsnachricht, die von einem Sender zu einem Empfänger gesendet wird, umfassend die Schritte:

(a) Setzen, auf der Senderseite, eines ersten privaten Schlüssels, der durch $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$ gegeben ist, eines ersten öffentlichen Schlüssels n, der durch ein Produkt $p_1^{k1} p_2^{k2} ... p_N^{kN}$ gegeben ist, wobei k1, k2, ... kN beliebig positive Ganzzahlen sind, eines zweiten öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod{L} \quad ,$$

wobei L das kleinste gemeinsame Vielfache von $p_1-1, p_2-1, ..., p_N-1$ ist;
(b) Erhalten, auf der Senderseite, eines Authentikators h(M) durch ein Zerhacken der Authentifizierungsnachricht M unter Verwendung einer Zerhackungsfunktion h;
(c) Erhalten, auf der Senderseite, eines verschlüsselten Authentikators h(C) des Authentikators h(M) gemäß:

$$h(M) = h(C)^e \pmod{n}$$

durch ein Erhalten von Residuen $h(C)_{p1k1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, jeweils des verschlüsselten Authentifikators h(C) unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels $p_1, p_2, ..., p_N$ und ein Anwenden des chinesischen Restsatzes auf Residuen $h(C)_{p1l1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$;
(d) Senden des verschlüsselten Authentifikators h(C) und der Authentifizierungsnachricht M von dem Sender zu dem Empfänger;
(e) Erhalten, auf der Empfängerseite, eines ersten Authentifikators $h(M)_1$ durch ein Berechnen von $h(C)^e \pmod{n}$ aus dem verschlüsselten Authentifikator h(C), der von dem Sender empfangen wird, unter Verwendung des zweiten öffentlichen Schlüssels e;
(f) Erhalten, auf der Empfängerseite, eines zweiten Authentifikators $h(M)_2$ durch ein Zerhacken der Authentifizierungsnachricht M, die von dem Sender empfangen wird, unter Verwendung der Zerhackungsfunktion h; und
(g) Beurteilen der Authentizität der Authentifizierungsnachricht M auf der Empfängerseite durch ein Überprüfen, ob der erste Authentifikator $h(M)_1$ und der zweite Authentifikator $h(M)_2$ übereinstimmen oder nicht;

dadurch gekennzeichnet, dass

der verschlüsselte Authentifikator h(C) unter Verwendung des ersten privaten Schlüssels, der durch zwei Primzahlen $p_1 = p$ und $p_2 = q$ gegeben ist, und den ersten öffentlichen Schlüssel n, der durch das Produkt $p^k q$ gegeben ist, wobei $k = k1$, erhalten wird;
der Schritt (c) ein Residuum $h(K)_\varnothing$ modulo p und ein Residuum $h(C)_q$ modulo q des verschlüsselten Authentifikators h(C) durch ganzzahlige modulare Exponentenberechnungen von:

$$h(K)_\varnothing := h(M)^{d\,p} \pmod{p};$$

und

$$h(C)_1 := h(M)^{d\ q} \pmod{q};$$

erhält, wobei:

$$dp := d \pmod{p-1};$$

und

$$dq := d \pmod{q-1};$$

und ein Residuum $h(C)_{pk}$ modulo p^k des verschlüsselten Authentifikators h(C) durch ein Anwenden der Schleifenberechnung auf $h(K)_{\varnothing}$ erhält, und den chinesischen Restsatz auf die Residuen $h(C)_{pk}$ und $h(C)_k$ anwendet; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $h(A)_{\varnothing} := h(K)_{\varnothing}$;
(b) für i = 1 bis (k - 1), wiederholtes Berechnen:

$$h(F)_i := (h(A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$h(E)_I := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1}\ h(A)_{i-1}\ h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

und
(c) Setzen von $h(C)_{pk} := h(A)_{k-1}$

6. Verfahren nach Anspruch 5, wobei der Schritt (c) den chinesischen Restsatz anwendet durch ein Berechnen:

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((h(C)_{p\ k} - h(C)_q)\ q_1) \pmod{p^k};$$

und

$$h(C) := (h(C)_q + qv_1).$$

7. Verfahren nach Anspruch 5, wobei der Schritt (c) den chinesischen Restsatz anwendet durch ein Berechnen:

$$p_1 := (p^k)^{-1} \pmod q;$$

$$q_1 := ((h(C)_q - h(C)_{p\,k})\ p_1) \pmod q;$$

und

$$h(C) := (h(C)_{p\,k} + p^k\ v_1).$$

8. Verfahren nach Anspruch 5, wobei der Schritt (c) den chinesischen Restsatz anwendet durch ein Berechnen:

$$p_1 := (p^k)^{-1} \pmod q;$$

$$q_1 := q^{-1} \pmod{p^k};$$

und

$$h(C) := (q_1\ qh(C)_{p\,k} + p_1\ p^k\ h(C)q) \pmod{p^k q}.$$

9. Entschlüsselungsvorrichtung zum Entschlüsseln eines Chiffre-Textes (C), der aus einem Klartext M erhalten wird, gemäß:

$$C = M^e \pmod n$$

unter Verwendung eines ersten privaten Schlüssels, der gegeben ist durch $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$, eines ersten öffentlichen Schlüssels n, der gegeben ist durch ein Produkt $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, wobei k1, k2, ..., kN beliebige positive Ganzzahlen sind, eines öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod L$$

wobei L das kleinste gemeinsame Vielfache von p_1-1, p_2-1, p_N-1 ist, wobei die Vorrichtung umfasst:

eine Berechnungsverarbeitungseinheit zum Erhalten von Residuen $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$ modulo p_1^{k1}, $p_2^{k2}, ..., p_N^{kN}$ jeweils des Klartextes M unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels $p_1, p_2, ..., p_N$; und
eine Entschlüsselungsverarbeitungseinheit zum Wiedergewinnen des Klartextes M durch ein Anwenden des chinesischen Restsatzes auf die Residuen $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$;

dadurch gekennzeichnet, dass

der Chiffre-Text C unter Verwendung des ersten privaten Schlüssels, der gegeben ist durch zwei Primzahlen $p_1 = p$ und $p_2 = q$, und des ersten öffentlichen Schlüssels n, der gegeben ist durch das Produkt $p^k q$, wobei k = k1, erhalten wird;
die Berechnungsverarbeitungseinheit ausgelegt ist, ein Residuum $K_\varnothing$ modulo p und ein Residuum M_q modulo

q des Klartextes M durch ganzzahlige modulare Exponentenberechnungen von:

$$K_{\varnothing} := C^{d\ p} \pmod{p};$$

und

$$M_q := C^{d\ q} \pmod{q};$$

zu erhalten, wobei:

$$dp := d \pmod{p-1};$$

und

$$dq := d \pmod{q-1};$$

und ausgelegt ist, ein Residuum M_{pk} modulo p^k des Klartextes M durch ein Anwenden der Schleifenberechnung auf $K_{\varnothing}$ zu erhalten; und
die WiedergewinnungsEntschlüsselungsVerarbeitungseinheit ausgelegt ist, den chinesischen Restsatz auf die Residuen M_{pk} und M_q anzuwenden; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $A_{\varnothing} := K_{\varnothing}$
(b) für i = 1 bis (k-1), wiederholtes Berechnen:

$$F_i := (A_{i-i}{}^{e}) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$Ki := ((eFi)^{-1}\ A_{i-1}\ B_i) \pmod{p};$$

$$Ai := A_{i-1} + p^i K_i \text{ in } Z;$$

und
(c) Setzen von $M_{pk} := A_{k-1}$

10. Chiffre-Kommunikationssystem, umfassend:

eine Sendervorrichtung, die aufweist:
eine Verschlüsselungs/Entschlüsselungs-Schlüsselerzeugungs-Verarbeitungseinheit zum Setzen von $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$ als einen ersten privaten Schlüssel, und ein Produkt $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$ als einen ersten öffentlichen Schlüssel n, wobei k1, k2, ..., kN beliebige positive Ganzzahlen sind, und zum Bestimmen

eines zweiten öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod{L}$$

wobei L das kleinste gemeinsame Vielfache von p_1-1, p_2-1, ..., p_N-1 ist, unter Verwendung des ersten privaten Schlüssels; und
eine Verschlüsselungsverarbeitungseinheit zum Erhalten eines Chiffre-Textes C aus einem Klartext M gemäß:

$$C = M^e \pmod{n}$$

unter Verwendung des ersten öffentlichen Schlüssels n und des zweiten öffentlichen Schlüssels e; und
eine Empfängervorrichtung, die aufweist:

eine Berechnungsverarbeitungseinheit zum Erhalten von Residuen M_{p1k1}, M_{p2k2}, ..., M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ..., p_n^{kN} jeweils des Klartextes M unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels p_1, p_2, ..., p_N; und
eine Entschlüsselungsverarbeitungseinheit zum Wiedergewinnen des Klartextes M durch ein Anwenden des chinesischen Restsatzes auf die Residuen M_{p1k1}, M_{p2k2}, ..., M_{pNkN};

dadurch gekennzeichnet, dass

der Chiffre-Text C unter Verwendung des ersten privaten Schlüssels, der gegeben ist durch zwei Primzahlen $p_1 = p$ und $p_2 = q$ und des ersten öffentlichen Schlüssels n, der gegeben ist durch das Produkt p^kq, wobei k = k1, erhalten wird;
die Berechnungsverarbeitungseinheit ausgelegt ist, ein Residuum $K_\varnothing$ modulo p und ein Residuum M_q modulo q des Klartestes M durch ganzzahlige modulare Exponentenberechnungen von:

$$K_\varnothing := C^d \; p \pmod{p};$$

und

$$M_q := C^d \; q \pmod{q};$$

zu erhalten, wobei:

$$dp := d \pmod{p-1};$$

und

$$dq := d \pmod{q-1};$$

und ausgelegt ist, ein Residuum M_{pk} modulo p^k des Klartextes M durch ein Anwenden der Schleifenberechnung auf $K_\varnothing$ zu erhalten; und
die Entschlüsselungsverarbeitungseinheit ausgelegt ist, den chinesischen Restsatz auf die Residuen M_{pk} und M_q anzuwenden; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $A_{\varnothing}$: = $K_{\varnothing}$
(b) für i = 1 bis (k-1), wiederholtes Berechnen:

$$F_i := (A_{i-i}{}^{e}) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$Ki := ((eFi)^{-1} Ai\text{-}1\ Bi) \pmod{p};$$

$$Ai := A_{i-1} + p^i K_i \text{ in } Z;$$

und
(c) Setzen von M_{pk}: = ^{A}k-1.

11. Authentifizierungsnachricht-Sendervorrichtung zur Verwendung beim Authentifizieren einer Authentifizierungsnachricht, die von einem Sender zu einem Empfänger gesendet wird, wobei die Vorrichtung umfasst:

eine Verschlüsselungs-/Entschlüsselungs-Schlüsselerzeugungsverarbeitungseinheit zum Setzen, auf der Senderseite, eines ersten privaten Schlüssels, der gegeben ist durch $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$, eines ersten öffentlichen Schlüssels n, der gegeben ist durch ein Produkt $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, wobei k1, k2, ..., kN beliebige positive Ganzzahlen sind, eines zweiten öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod{L}$$

wobei L das kleinste gemeinsame Vielfache von p_1-1, P_2-1, ..., P_N-1 ist;
eine Authentifizierungsnachricht-Zerhackungsverarbeitungseinheit zum Erhalten, auf der Senderseite, eines Authentifikators h(M) durch ein Zerhacken der Authentifizierungsnachricht M unter Verwendung einer Zerhakkungsfunktion h; und
eine Authentifizierungs-Verschlüssungs-Verarbeitungseinheit zum Erhalten, auf der Senderseite, eines verschlüsselten Authentifikators h(C) des Authentifikators h(M) gemäß:

$$h(M) = h(C)^{e} \pmod{n}$$

durch ein Erhalten von Residuen $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$ jeweils des verschlüsselten Authentifikators h(C) unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels $p_1, p_2, ..., p_N$ und durch ein Anwenden des chinesischen Restsatzes auf die Residuen $h(C)_{p1k1}$, h $(C)_{p2k2}$, ..., $h(C)_{pNkN}$ und dann ein Senden des verschlüsselten Authentifikators h(C) und der Authentifikationsnachricht M zu dem Empfänger;

dadurch gekennzeichnet, dass

der verschlüsselte Authentifikator h(C) unter Verwendung des ersten privaten Schlüssels, der gegeben ist durch

zwei Primzahlen $p_1 = p$ und $p_2 = q$ und des ersten öffentlichen Schlüssels n, der gegeben ist durch das Produkt $p^k q$, wobei k = k1, erhalten wird;
die Authentifizierungs-VerschlüsselungsVerarbeitungseinheit ausgelegt ist, ein Residuum $h(K)_{\varnothing}$ modulo p und ein Residuum $h(C)_q$ modulo q des verschlüsselten Authentifikators h(C) durch ganzzahlige modulare Exponentenberechnungen von:

$$h(K)_{\varnothing} := h(M)^d \ p \pmod{p};$$

und

$$h(C)_1 := h(M)^d \ q \pmod{q};$$

zu erhalten, wobei:

$$dp := d \pmod{p-1};$$

und

$$dq := d \pmod{q-1};$$

und ausgelegt ist, ein Residuum $h(C)_{pk}$ modulo p^k des verschlüsselten Authentifikators h(C) durch ein Anwenden der Schleifenberechnung auf $h(K)_{\varnothing}$ zu erhalten und den chinesischen Restsatz auf die Residuen $h(C)_{pk}$ und $h(C)_q$ anzuwenden; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $h(A)_{\varnothing} := h(K)_{\varnothing}$;
(b) für i = 1 bis (k - 1), wiederholtes Berechnen:

$$h(F)_i := (h(A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i := h(E)_i / p^i \text{ in } Z;$$

$$h(K)_i := ((eh(F)_i)^{-1} \ h(A)_{i-1} \ h(B)_i) \pmod{p};$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

und
(c) Setzen von $h(C)_{pk} := h(A)_{k-1}$.

12. Authentifizierungssystem zur Authentifizierung einer Authentifizierungsnachricht, die von einen Sender zu einem Empfänger gesendet wird, wobei das System umfasst:

eine Sendervorrichtung, die aufweist:

eine Verschlüsselungs-/Entschlüsselungs-Schlüsselerzeugungsverarbeitungseinheit zum Setzen, auf der Senderseite, eines ersten privaten Schlüssels, der gegeben ist durch $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$, eines ersten öffentlichen Schlüssels n, der gegeben ist durch ein Produkt $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, wobei k1, k2, ..., kN beliebige positive Ganzzahlen sind, eines zweiten öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod{L}$$

wobei L das kleinste gemeinsame Vielfache von $p_1-1, p_2-1, ..., p_N-1$ ist;
eine Authentifizierungsnachricht-Zerhackungsverabeitungseinheit zum Erhalten, auf der Senderseite, eines Authentifikators h(M) durch ein Zerhacken der Authentifizierungsnachricht M unter Verwendung einer Zerhakkungsfunktion h; und
eine Authentifizierungs-Verschlüssungs-Verarbeitungseinheit zum Erhalten, auf der Senderseite, eines verschlüsselten Authentifikators h(C) des Authentifikators h(M) gemäß:

$$h(M) = h(C)^e \pmod{n}$$

durch ein Erhalten von Residuen $h(C)_{p1k1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$ jeweils des verschlüsselten Authentifikators h(C) unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels $p_1, p_2, ..., p_N$ und durch ein Anwenden des chinesischen Restsatzes auf die Residuen $h(C)_{p1k1}, h(C)_{p2k2}, ..., h(C)_{pNkN}$ und dann ein Senden des verschlüsselten Authentifikators h(C) und der Authentifikationsnachricht M zu dem Empfänger; und
eine Empfängervorrichtung, die aufweist:

eine AuthentifikatorEntschlüsselungsVerarbeitungseinheit zum Erhalten eines ersten Authentifikators $h(M)_1$ durch ein Berechnen von $h(C)^e \pmod{n}$ aus dem entschlüsselten Authentifikator h(C), der von dem Sender empfangen wird, unter Verwendung des zweiten öffentlichen Schlüssels e;
eine Authentifizierungsnachricht-Zerhackungsverarbeitungseinheit zum Erhalten eines zweiten Authentifikators $h(M)_2$ durch ein Zerhacken der Authentifizierungsnachricht, die von dem Sender empfangen wird, unter Verwendung der Zerhackungsfunktion h; und
eine Authentizitäts-Verifikations-Verarbeitungseinheit zum Beurteilen der Authentifizität der Authentifizierungsnachricht M durch ein Überprüfen, ob der erste Authentifikator $h(M)_1$ und der zweite Authentifikator $h(M)_2$ übereinstimmen oder nicht;

dadurch gekennzeichnet, dass

der verschlüsselte Authentifikator h(C) unter Verwendung des ersten privaten Schlüssels, der gegeben ist durch zwei Primzahlen $p_1 = p$ und $p_2 = q$, und des ersten öffentlichen Schlüssels n, der gegeben ist durch das Produkt $p^k q$, wobei $k = k1$, erhalten wird;
die AuthentifizierungsVerschlüsselungsVerarbeitungseinheit ausgelegt ist, ein Residuum $h(K)_\varnothing$ modulo p und ein Residuum $h(C)_1$ modulo q des verschlüsselten Authentifikators h(C) durch ganzzahlige modulare Exponentenberechnungen von:

$$h(K)_\varnothing := h(M)^{d\,p} \pmod{p};$$

und

$$h(C)_q := h(M)^{d\,q} \pmod{q};$$

zu erhalten, wobei:

$$dp: = d \pmod{p-1};$$

und

$$dq: = d \pmod{q-1};$$

und ausgelegt ist, ein Residuum $h(C)_{pk}$ modulo p^k des verschlüsselten Authentifikators h(C) durch ein Anwenden der Schleifenberechnung auf $h(K)_{\varnothing}$ zu erhalten und den chinesischen Restsatz auf die Residuen $h(C)_{pk}$ und $h(C)_q$ anzuwenden; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $h(A)_{\varnothing}: = h(K)_{\varnothing}$;
(b) für i = 1 bis (k - 1), wiederholtes Berechnen:

$$h(F)_i: = (h(A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$h(E)_i: = (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i: = h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i: = ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i: = h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

und
(c) Setzen von $h(C)_{pk}: = h(A)_{k-1}$.

13. Computer-verwendbares Medium, das eine computerlesbare Programmcodeeinrichtung darin enthalten aufweist, um einen Computer zu veranlassen, als eine Entschlüsselungsvorrichtung zum Entschlüsseln eines Chiffre-Textes C zu arbeiten, der aus einem Klartext M erhalten wird, gemäß:

$$C = M^e \pmod{n}$$

unter Verwendung eines ersten privaten Schlüssels, der gegeben ist durch $N \geq 2$ Primzahlen $p_1, p_2, ..., p_N$, eines ersten öffentlichen Schlüssels n, der gegeben ist durch ein Produkt $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, wobei k1, k2, ..., k_N beliebige positive Ganzzahlen sind, eines zweiten öffentlichen Schlüssels e und eines zweiten privaten Schlüssels d, die erfüllen:

$$ed = 1 \pmod{L}$$

wobei L das kleinste gemeinsam Vielfache von $p_1-1, p_2-1, ..., p_N-1$ ist, wobei die erste Computer-lesbare Programmcodeeinrichtung einschließt:

eine erste computerlesbare Programmcodeeinrichtung zum Herbeiführen, dass der Computer Residuen M_{p1k1}, M_{p2k2}, ..., M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN} jeweils des Klartextes M unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels p_1, p_2, ..., p_N erhält; und
eine zweite computerlesbare Programmcodeeinrichtung zum Herbeiführen, dass der Computer den Klartext M durch ein Anwenden des chinesischen Restsatzes auf die Residuen M_{p1k1}, M_{p2k2}, ..., M_{pNkN} wiedergewinnt;

dadurch gekennzeichnet, dass

der Chiffre-Text C unter Verwendung des ersten privaten Schlüssels, der gegeben ist durch zwei Primzahlen $p_1 = p$ und $p_2 = q$ und den ersten öffentlichen Schlüssel n, der gegeben ist durch das Produkt $p^k q$, wobei $k = k_1$, erhalten wird;
die erste computerlesbare Programmcodeeinrichtung ein Residuum $K_\varnothing$ modulo p und ein Residuum M_1 modulo q des Klartextes M durch ganzzahlige modulare Exponentenberechnungen von:

$$K_\varnothing := C^d \; p \pmod{p};$$

und

$$M_q := C^d \; q \pmod{q};$$

erhält, wobei:

$$dp := d \pmod{p-1};$$

und

$$dq := d \pmod{q-1};$$

und ein Residuum M_{pk} modulo p^k des Klartextes M durch ein Anwenden der Schleifenberechnungen auf $K_\varnothing$ erhält; und
die zweite computerlesbare Programmcodeeinrichtung den chinesischen Restsatz auf die Residuen M_{pk} und M_q anwendet; und
die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $A_\varnothing := K_\varnothing$;
(b) für i = 1 bis (k - 1), wiederholtes Berechnen:

$$F_i := (A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$E_i := (C - F_i) \pmod{p^{i+1}};$$

$$B_i := E_i/p^i \text{ in } Z;$$

$$K_i := ((eF_i)^{-1} \; A_{i-1} \; B_i) \pmod{p};$$

$$A_i := A_{i-1} + p^i K_i \text{ in } Z;$$

und

(c) Setzen von M_{pk}: = A_{k-1}.

14. Computer-verwendbares Medium, das eine computerlesbare Programmcodeeinrichtung darin enthalten aufweist, um einen Computer zu veranlassen, als eine Authentifizierungsnachricht-Sendervorrichtung zur Verwendung beim Authentifizieren einer Authentifizierungsnachricht zu arbeiten, die von einem Sender zu einem Empfänger gesendet wird, wobei die computerlesbare Programmcodeeinrichtung einschließt:

eine erste computerlesbare Programmcodeeinrichtung zum Herbeiführen, dass der Computer auf der Senderseite einen ersten privaten Schlüssel, der gegeben ist durch N ≥ 2 Primzahlen p_1, p_2, ..., p_N, einen ersten öffentlichen Schlüssel n, der gegeben ist durch ein Produkt p_1^{k1} p_2^{k2} .... p_N^{kN}, wobei k1, k2, ..., kN beliebige positive Ganzzahlen sind, einen zweiten öffentlichen Schlüssel e und einen zweiten privaten Schlüssel d, die erfüllen:

$$ed = 1 \pmod{L}$$

setzt, wobei L das kleinste gemeinsame Vielfache von p_1-1, p_2-1, P_N-1 ist;
eine zweite computerlesbare Programmcodeeinrichtung zum Herbeiführen, dass der Computer auf der Senderseite einen Authentifikator h(M) durch ein Zerhacken der Authentifizierungsnachricht M unter Verwendung einer Zerhackungsfunktion h erhält; und
eine dritte computerlesbare Programmcodeeinrichtung zum Herbeiführen, dass der Computer auf der Senderseite einen verschlüsselten Authentifikator h(C) des Authentifikators h(M) gemäß:

$$h(M) = h(C)^e \pmod{n}$$

durch ein Erhalten von Residuen $h(C)_{p1k1}$, $h(C)_{p2k2}$, ...$h(C)_{pNkN}$ modulo p_1^{k1}, P_2^{k2}, ..., p_N^{kN} jeweils des verschlüsselten Authentifikators h(C) unter Verwendung einer Schleifenberechnung bezüglich des ersten privaten Schlüssels p_1, p_2, ..., p_N und ein Anwenden des chinesischen Restsatzes auf die Residuen $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ und dann durch ein Senden des verschlüsselten Authentifikators h(C) und der Authentifizierungsnachricht M zu dem Empfänger erhält;

dadurch gekennzeichnet, dass

der verschlüsselte Authentifikator h(C) unter Verwendung des ersten privaten Schlüssels, der gegeben ist durch zwei Primzahlen p_1 = p und p_2 = q und des ersten öffentlichen Schlüssels n, der gegeben ist durch das Produkt p^kq, wobei k = k1, erhalten wird;
die dritte lesbare Programmcodeeinrichtung ein Residuum $h(K)_\varnothing$ modulo p und ein Residuum $h(C)_q$ modulo q des verschlüsselten Authentifikators h(C) durch ganzzahlige modulare Exponentenberechnungen von:

$$h(K)_\varnothing := h(M)^{d\,p} \pmod{p};$$

und

$$h(C)_q := h(M)^{d\,q} \pmod{q};$$

erhält, wobei:

$$dp := d \pmod{p-1};$$

und

$$dq: = d \pmod{q-1};$$

und ein Residuum $h(C)p_k$ modulo p^k des verschlüsselten Authentifikators h(C) durch ein Anwenden der Schleifenberechnung auf $h(K)_{\varnothing}$ erhält und den chinesischen Restsatz auf die Residuen $h(C)_{pk}$ und $h(C)_q$ anwendet; und die Schleifenberechnung ausgeführt wird durch:

(a) Setzen von $h(A)_{\varnothing} := h(K)_{\varnothing}$;
(b) für i = 1 bis (k - 1); wiederholtes Berechnen:

$$h(F)_i: = (h(A)_{i-1}{}^e) \pmod{p^{i+1}};$$

$$h(E)_i: = (h(M) - h(F)_i) \pmod{p^{i+1}};$$

$$h(B)_i: = h(E)_i/p^i \text{ in } Z;$$

$$h(K)_i: = ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$

$$h(A)_i: = h(A)_{i-1} + p^i h(K)_i \text{ in } Z;$$

und
(c) Setzen von $h(C)_{pk} := h(A)_{k-1}$.

Revendications

1. Procédé de déchiffrage pour déchiffrer un texte chiffré C obtenu à partir d'un texte en clair M en conformité avec :

$$C \equiv M^e \pmod{n}$$

en utilisant une première clé privée donnée par $N \geq 2$ de nombres premiers $p_1, p_2, ..., p_N$, une première clé publique n donnée par un produit $p_1{}^{k1}, p2^{k2}, ..., p_N{}^{kN}$ où k1, k2, ..., kN sont des nombres entiers positifs arbitraires, une seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le plus petit commun multiple de p_1-1, p_2-1, ..., p_N-1, le procédé comprenant les étapes consistant à :

obtenir des résidus $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$ modulo $p_1{}^{k1}, p_2{}^{k2}, ..., p_N{}^{kN}$, respectivement, du texte en clair M en utilisant un calcul en boucle par rapport à la première clé privée $p_1, p_2, ..., p_N$; et
reconstituer le texte en clair M en appliquant le théorème du reste chinois aux résidus $M_{p1k1}, M_{p2k2}, ..., M_{pNkN}$;

CARACTERISE EN CE QUE

le texte chiffré C est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et $p_2 = q$ et la première clé publique n procurée par le produit $p^k q$ où $k = k1$;
l'étape d'obtention obtient un résidu K_0 modulo p et un résidu M_q modulo q du texte en clair M par le calcul d'exposant modulaire entier de :

$$K_0 := C^{dp} \pmod{p} ;$$

et

$$M_q := C^{dq} \pmod{q}$$

où :

$$dp := d \pmod{p-1} ;$$

et

$$dq = d \pmod{q-1}$$

et obtient un résidu M_{pk} modulo p^k du texte en clair M en appliquant le calcul en boucle à K_0 ; et les étapes de reconstitution appliquent le théorème de reste chinois aux résidus M_{pk} et M_q ; et le calcul en boucle est effectué par :

(a) établir $A_0 := K_0$;
(b) pour i = 1 à (k-1), calculer de manière répétée :

$$F_i := (A_{i-1}{}^e) \pmod{p^{i+1}} ;$$

$$E_i := (C - F_i) \pmod{p^{i+1}} ;$$

$$B_i := E_i/p^i \text{ dans } Z ;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p} ;$$

$$A_i := A_{i-1} + p^i K_i \text{ dans } Z ;$$

et
(c) établir $M_{pk} := A_{k-1}$.

2. Procédé selon la revendication 1, dans lequel l'étape de reconstitution reconstitue le texte en clair M en calculant :

$$q_1 := q^{-1} \pmod{p^k} ;$$

$$V_1 := ((M_{pk} - M_q)\, q_1) \pmod{p^k} ;$$

et

$$M := (M_q + q v_1) .$$

3. Procédé selon la revendication 1, dans lequel l'étape de reconstitution reconstitue le texte en clair M en calculant :

$$p_1 := (p^k)^{-1} \pmod{q} ;$$

$$V_1 := ((M_q - M_{pk})\, p_1) \pmod{q} ;$$

et

$$M := (M_{pk} + p^k\, v_1) .$$

4. Procédé selon la revendication 1, dans lequel l'étape de reconstitution reconstitue le texte en clair M en calculant :

$$p_1 := (p^k)^{-1} \pmod{q} ;$$

$$q_1 := q^{-1} \pmod{p^k} ;$$

et

$$M := (q_1\, q M_{pk} + p_1\, p^k\, M_q) \pmod{p^k q} .$$

5. Procédé d'authentification pour authentifier un message d'authentification envoyé d'un émetteur à un récepteur, comprenant les étapes consistant à :

(a) établir au niveau du côté émetteur une première clé privée procurée par $N \geq 2$ nombres premiers $p_1, p_2, \ldots, p_N$, une première clé publique procurée par le produit $p_1^{k1}\, p_2^{k2} \ldots p_N^{kN}$ où k1, k2, ... kN sont des nombres entiers positifs arbitraires, une seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le plus petit commun multiple de $p_1-1, p_2-1, \ldots, P_N-1$;
(b) obtenir au niveau du côté émetteur un authentificateur h(M) en hachant le message d'authentification M en utilisant une fonction de hachage h ;
(c) obtenir au niveau du côté émetteur un authentificateur chiffré h(C) de l'authentificateur h(M) en conformité avec :

$$h(M) \equiv h(C)^e \pmod{n}$$

en obtenant les résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ... , $h(C)_{pNkN}$ module p_1^{k1}, p_2^{k2}, ..., p_N^{kN}, respectivement de l'authentificateur chiffré h(C) en utilisant un calcul en boucle par rapport à la première clé privée p_1, p_2, ..., p_N, et appliquer le théorème de reste chinois aux résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$;
(d) émettre l'authentificateur chiffré h(C) et le message d'authentification M de l'émetteur au récepteur ;
(e) obtenir au niveau du côté récepteur, un premier authentificateur $h(M)_1$ en calculant $h(C)^e$ (mod n) depuis l'authentificateur chiffré h(C) reçu de l'émetteur en utilisant la seconde clé publique e ;
(f) obtenir au niveau du côté récepteur un second authentificateur $h(M)_2$ en hachant le message d'authentification M reçu de l'émetteur en utilisant la fonction de hachage h ; et
(g) juger de l'authenticité du message d'authentification M au niveau du côté récepteur en vérifiant si le premier authentificateur $h(M)_1$ et le second authentificateur $h(M)_2$ coïncident ou non ;

CARACTERISE EN CE QUE

l'authentificateur chiffré h(C) est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et $p_2 = q$ et la première clé publique n procurée par le produit p^kq où $k = k1$;
l'étape (c) obtient un résidu $h(K)_0$ modulo p et un résidu $h(C)_q$ modulo q de l'authentificateur chiffré h(C) par des calculs d'exposant modulaire d'entier de :

$$h(K)_0 := h(M)^{dp} \pmod{p} ;$$

et

$$h(C)_q := h(M)^{dq} \pmod{q} ;$$

où :

$$dp := d \pmod{p-1} ;$$

et

$$dq := d \pmod{q-1} ;$$

et obtient un résidu $h(C)_{pk}$ modulo p^k de l'authentificateur chiffré h(C) en appliquant le calcul en boucle à $h(K)_0$, et applique le théorème de reste chinois aux résidus $h(c)_{pk}$ et $h(C)_q$; et
le calcul en boucle est effectué par :

(a) établir $h(A)_0 := h(K)_0$;
(b) pour i = 1 à (k-1), calculer de manière répétée :

$$h(F)_i := (h(A_{i-1}^e) \pmod{p^{i+1}}) ;$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}} ;$$

$$h(B)_i := h(E)_i/p^i \text{ dans } Z ;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p} ;$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ dans } Z ;$$

et

(c) établir $h(C)_{pk} := h(A)_{k-1}$.

6. Procédé selon la revendication 5, dans lequel l'étape (c) applique le théorème de reste chinois en calculant :

$$q_1 := q^{-1} \pmod{p^k} ;$$

$$v_1 := ((h(C)_{pk} - h(C)_q) q_1) \pmod{p^k} ;$$

et

$$h(C) := (h(C)_q + qv_1) .$$

7. Procédé selon la revendication 5, dans lequel l'étape (c) applique le théorème de reste chinois en calculant :

$$p_1 := (p^k)^{-1} \pmod{q} ;$$

$$v_1 := ((h(C)_q - h(C)_{pk}) p_1) \pmod{q} ;$$

et

$$h(C) := (h(C)_{pk} + p^k v_1) .$$

8. Procédé selon la revendication 5, dans lequel l'étape (c) applique le théorème de reste chinois en calculant :

$$p_1 := (p^k)^{-1} \pmod{q} ;$$

$$q_1 := q^{-1} \pmod{p^k} ;$$

et

$$h(C) := (q_1 qh(C)_{pk} + p_1 p^k h(C)q) \pmod{p^k q} .$$

9. Appareil de déchiffrage pour déchiffrer un texte chiffré C obtenu à partir d'un texte ordinaire M en conformité avec :

$$C \equiv M^e \pmod{n}$$

en utilisant une première clé privée procurée par N≥2 nombres premiers p_1, p_2, ..., p_N, une première clé publique n procurée par un produit $p_1^{k1} p_2^{k2} ... p_N^{kN}$ où k1, k2, ..., kN sont des nombres entiers positifs arbitraires, une

seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le plus petit commun multiple de p_1-1, p_2-1, ..., p_N-1, l'appareil comprenant :

une unité de traitement de calcul pour obtenir des résidus M_{p1k1}, M_{p2k2}, ... M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN} respectivement du texte en clair M en utilisant un calcul en boucle par rapport à la première clé privée p_1, p_2, ..., p_N ; et
une unité de traitement de déchiffrage pour reconstituer le texte en clair M en appliquant le théorème de reste chinois aux résidus M_{p1k1}, M_{p2k2}, ... M_{pNkN} ;

CARACTERISE EN CE QUE

le texte chiffré C est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et p2 = q et la première clé publique n procurée par le produit $p^k q$ où k = k1 ;
l'unité de traitement de calcul est adaptée pour obtenir un résidu K_0 modulo p et un résidu M_q modulo q du texte en clair M, par des calculs d'exposant modulaire d'entier de :

$$K_0 := C^{dp} \pmod{p} ;$$

et

$$M_q := C^{dq} \pmod{q} ;$$

où

$$dp := d \pmod{p-1} ;$$

et

$$dq = d \pmod{q-1} ;$$

et est adaptée pour obtenir un résidu M_{pk} modulo p^k du texte en clair M en appliquant le calcul en boucle à K_0 ; et l'unité de traitement de déchiffrage de reconstitution est adaptée pour appliquer le théorème de reste chinois aux résidus M_{pk} et M_q ; et
le calcul en boucle est effectué par :

(a) établir $A_0 := K_0$;
(b) pour i = 1 à (k-1), calculer de manière répétée :

$$F_i := (A_{i-1}^e) \pmod{p^{i+1}} ;$$

$$E_i := (C - F_i) \pmod{p^{i+1}} ;$$

$$B_i := E_i/p^i \text{ dans } Z ;$$

$$K_i := ((eF_i)^{-1})\ A_{i-1}\ B_i)\ (\text{mod } p)\ ;$$

$$A_i := A_{i-1} + p^i\ K_i \text{ dans } Z\ ;$$

et
(c) établir $M_{pk} := A_{k-1}$.

10. Système de communication chiffré, comprenant :

un appareil émetteur ayant :

une unité de traitement de génération de clés de chiffrage/déchiffrage pour établir N ≥ 2 nombres premiers p1, p2, ..., p_N comme première clé privée, et un produit $p_1^{k1}\ p_2^{k2}$ ...., p_N^{kN} comme première clé publique n, où k1, , k2, ..., kN sont des nombres entiers positifs arbitraires, et déterminer une seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1\ (\text{mod } L)$$

où L est le plus petit commun multiple de p_1-1, p_2-1, ..., p_N-1, en utilisant la première clé privée ; et
une unité de traitement de chiffrage pour obtenir un texte chiffré C à partir d'un texte en clair M en conformité avec :

$$C \equiv M^e\ (\text{mod } n)$$

en utilisant la première clé publique n et la seconde clé publique e ; et

un appareil récepteur ayant :

une unité de traitement de calcul pour obtenir des résidus M_{p1k1}, M_{p2k2}, ... M_{pNkN} module p_1^{k1}, p^{k2}, ..., p_N^{KN} respectivement, du texte en clair M en utilisant un calcul en boucle par rapport à la première clé privée p_1, p_2, ..., p_N ; et
une unité de traitement de déchiffrage pour reconstituer le texte en clair M en appliquant le théorème de reste chinois aux résidus M_{p1k1}, M_{p2k2}, ... M_{pNkN} ;

CARACTERISE EN CE QUE

le texte chiffré C est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et p2 = q et la première clé publique n procurée par le produit p^kq où k = k1 ;
l'unité de traitement de calcul est adaptée pour obtenir un résidu K_0 modulo p et un résidu M_q modulo q du texte ordinaire M, par des calculs d'exposant modulaire entier de :

$$K_0 := C^{dp}\ (\text{mod } p)\ ;$$

et

$$M_q := C^{dq}\ (\text{mod } q)\ ;$$

où

$$dp := d \pmod{p-1} ;$$

et

$$dq = d \pmod{q-1} ;$$

et est adaptée pour obtenir un résidu M_{pk} modulo p^k du texte en clair M en appliquant le calcul en boucle à K_0 ; et l'unité de traitement de déchiffrage est adaptée pour appliquer le théorème de reste chinois aux résidus M_{pk} et M_q ; et
le calcul en boucle est effectué par :

(a) établir $A_0 : K_0$;
(b) pour i = 1 à (k-1), calculer de manière répétée :

$$F_i := (A_{i-1}{}^e) \pmod{p^{i+1}} ;$$

$$E_i := (C - F_i) \pmod{p^{i+1}} ;$$

$$B_i := E_i/p^i \text{ dans } Z ;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p} ;$$

$$A_i := A_{i-1} + p^i K_i \text{ dans } Z ;$$

et
(c) établir $M_{pk} := A_{k-1}$.

11. Appareil émetteur de message d'authentification pour utilisation dans l'authentification d'un message d'authentification émis depuis un émetteur vers un récepteur, l'appareil comprenant :

une unité de traitement de génération de clés de chiffrage/déchiffrage pour établir au niveau du côté émetteur une première clé privée procurée par $N \geq 2$ nombres premiers p1, p2, ..., p_N, une première clé publique n procurée par un produit $p_1{}^{k1}\ p_2{}^{k2} \ldots p_N{}^{kN}$ où k1, k2, ..., kN sont des nombres entiers positifs arbitraires, une seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le plus petit commun multiple de p_1-1, p_2-1, ..., P_N-1 ;
une unité de traitement de hachage de message d'authentification pour obtenir au niveau du côté émetteur un authentificateur h(M) en hachant le message d'authentification M en utilisant une fonction de hachage h ; et
une unité de traitement de chiffrage d'authentificateur pour obtenir au niveau du côté émetteur un authentificateur chiffré h(C) de l'authentificateur h(M) en conformité avec :

$$h(M) \equiv h(C)^e \pmod{n}$$

en obtenant les résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ... $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ... p_N^{kN} respectivement, de l'authentificateur chiffré h(C) en utilisant un calcul en boucle par rapport à la première clé privée p_1, p_2, ..., P_N et en appliquant le théorème de reste chinois aux résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{PNkN}$ et en émettant ensuite l'authentificateur chiffré h(C) et le message d'authentification M vers le récepteur ;

CARACTERISE EN CE QUE

l'authentificateur chiffré h(C) est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et $p2 = q$ et la première clé publique n procurée par le produit $p^k q$ où k = k1 ;
l'unité de traitement de chiffrage d'authentification est adaptée pour obtenir un résidu $h(K)_0$ modulo p et un résidu $h(C)_q$ modulo q de l'authentificateur chiffré h(C), par des calculs d'exposant modulaire d'entier de :

$$h(K)_0 := h(M)^{dp} \pmod{p} ;$$

et

$$h(C)_q := h(M)^{dq} \pmod{q} ;$$

où

$$dp := d \pmod{p-1} ;$$

et

$$dq = d \pmod{q-1} ;$$

et est adaptée pour obtenir un résidu $h(C)_{pk}$ modulo p^k de l'authentificateur chiffré h(C) en appliquant le calcul en boucle à $h(K)_0$, et est adaptée pour appliquer le théorème de reste chinois aux résidus $h(C)_{pk}$ et $h(C)_q$; et le calcul en boucle est effectué par :

(a) établir $h(A)_0 := h(K)_0$;
(b) pour i = 1 à (k-1), calculé de manière répétée :

$$h(F)_i := (h(A)_{i-1}^e) \pmod{p^{i+1}} ;$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}} ;$$

$$h(B)_i := h(E)_i / p^i \text{ dans } Z ;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p} ;$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ dans } Z ;$$

et
(c) établir $h(C)_{pk} := h(A)_{k-1}$.

12. Système d'authentification pour authentifier un message d'authentification émis depuis un émetteur vers un récepteur, le système comprenant :

un appareil émetteur ayant :

une unité de traitement de génération de clé de chiffrage/déchiffrage pour établir au niveau du côté émetteur une première clé privée procurée par $N \geq 2$ nombres premiers $p_1, p_2, \ldots, p_N$; une première clé publique n procurée par un produit $p_1^{k1}, p_2^{k2}, \ldots, p_N^{kN}$ où k1, k2, ..., kN sont des nombres entiers positifs arbitraires, une seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le multiplicateur le moins commun de $p_1-1, p_2-1, \ldots, p_N-1$;
une unité de traitement de hachage de message d'authentification pour obtenir au niveau du côté émetteur un authentificateur (M) en hachant le message d'authentification M en utilisant une fonction de hachage h ; et une unité de traitement de chiffrage d'authentificateur pour obtenir au niveau du côté émetteur un authentificateur chiffré h(C) de l'authentificateur h(M) en conformité avec :

$$h(M) \equiv h(C)^e \pmod{n}$$

en obtenant les résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \ldots, p_N^{kN}$, respectivement de l'authentificateur chiffré h(C) en utilisant un calcul en boucle par rapport à la première clé privée $p_1, p_2, \ldots, p_N$ et en appliquant le théorème de reste chinois aux résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ et en émettant ensuite l'authentificateur chiffré h(C) et le message d'authentification M vers le récepteur ; et

un appareil récepteur ayant :

une unité de traitement de déchiffrage d'authentificateur pour obtenir un premier authentificateur $h(M)_1$ par le calcul de $h(C)^e \pmod{n}$ depuis l'authentificateur chiffré h(C) reçu de l'émetteur en utilisant la seconde clé publique e ;
une unité de traitement de hachage de message d'authentification pour obtenir un second authentificateur $h(M)_2$ en hachant le message d'authentification M reçu de l'émetteur en utilisant la fonction de hachage h ; et une unité de traitement de vérification d'authenticité pour juger de l'authenticité du message d'authentification M en vérifiant si le premier authentificateur $h(M)_1$ et le second authentificateur $h(M)_2$ coïncident ou non ;

CARACTERISE EN CE QUE

l'authentificateur chiffré h(C) est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et $p_2 = q$ et la première clé publique n procurée par le produit $p^k q$ où $k = k1$;
l'unité de traitement de chiffrage d'authentification est adaptée pour obtenir un résidu $h(K)_0$ modulo p et un résidu $h(k)_0$ modulo q de l'authentificateur chiffré h(C) par les calculs d'exposant modulaire d'entier de :

$$h(K)_0 := h(M)^{dp} \pmod{p} ;$$

et

$$h(C)q := h(M)^{dq} \pmod{q} ;$$

où

$$dp := d \pmod{p-1} ;$$

et

$$dq := d \pmod{q-1} ;$$

et est adapté pour obtenir un résidu $h(C)_{pk}$ modulo p^k de l'authentificateur chiffré h(C) en appliquant le calcul en boucle à $h(K)_0$, et est adapté pour appliquer le théorème de reste chinois aux résidus $h(C)_{pk}$ et $h(C)_q$; et le calcul en boucle est effectué par :

(a) établir $h(C)_0 := h(K)_0$;
(b) pour i = 1 à (k-1), calculé de manière répétée :

$$h(F)_i := (h(A)_{i-1}^e) \pmod{p^{i+1}} ;$$

$$h(E)_i := (h(M) - h(F)_i) \bmod p^{i+1}) ;$$

$$h(B)_i := h(E)_i/p^i \text{ dans } Z ;$$

$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p} ;$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ dans } Z ;$$

et
(c) établir $h(C)_{pk} := h(A)_{k-1}$.

13. Support utilisable pour ordinateur ayant un moyen de code programme lisible par ordinateur incorporé dans celui-ci pour amener un ordinateur à fonctionner comme appareil de déchiffrage pour déchiffrer un texte chiffré C obtenu à partir d'un texte en clair M en conformité avec :

$$C \equiv M^e \pmod{n}$$

en utilisant une première clé privée procurée par $N \geq 2$ nombres premiers $p_1, p_2, ..., p_N$, une première clé publique n procurée par un produit $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$ où k1, k2, ..., kN sont des nombres entiers positifs arbitraires, une seconde clé publique e et une seconde clé privée d qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le plus petit commun multiple de $p_1-1, p_2-1, ..., p_N-1$, le moyen de code programme lisible par ordinateur inclut :

un premier moyen de code programme lisible par ordinateur pour amener ledit ordinateur à obtenir les résidus $Mp_{1k1}, Mp_{2k2}, ..., M_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, ..., p_N^{kN}$, respectivement, du texte en clair M en utilisant un calcul en boucle par rapport à la première clé privée $p_1, p_2, ..., p_N$; et
un second moyen de code programme lisible par ordinateur pour amener ledit ordinateur à reconstituer le texte en clair M en appliquant le programme de reste chinois aux résidus $Mp_{1k1}, Mp_{2k2}, ..., Mp_{NkN}$;

CARACTERISE EN CE QUE

le texte chiffré C est obtenu en utilisant la première clé privée procurée par deux nombres premiers $p_1 = p$ et $p_2 = q$ et la première clé publique n procurée par le produit p^kq où k = k1 ;
le premier moyen de code programme lisible par ordinateur obtient un résidu K_0 modulo p et un résidu M_q

modulo q du texte en clair M, par les calculs d'exposant modulaire d'entier de :

$$k_0 := C^{dp} \pmod{p} ;$$

et

$$Mq := C^{dq} \pmod{q} ;$$

où

$$dp := d \pmod{p-1}$$

et

$$dq := d \pmod{q-1} ;$$

et obtient un résidu M_{pk} modulo p^k du texte ordinaire M en appliquant le calcul en boucle k_0 ; et
le second moyen de code programme lisible par ordinateur applique le théorème de reste chinois aux résidus Mp_k et M_q ; et
le calcul en boucle est effectué par :

(a) établir $A_0 : k_0$;
(b) pour i = 1 à (k-1), calculé de manière répétée :

$$Fi := (A_{i-1}{}^e) \pmod{p^{i+1}} ;$$

$$E_i := (C - F_i) \pmod{p^{i+1}} ;$$

$$B_i := E_i/p^i \text{ dans } Z ;$$

$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p} ;$$

$$A_i := A_{i-1} + p^i k_i \text{ dans } Z ;$$

et
(c) établir $M_{pk} := A_{k-1}$.

14. Support utilisable par ordinateur ayant un moyen de code programme lisible par ordinateur incorporé dans celui-ci pour amener un ordinateur à fonctionner comme appareil émetteur de message d'authentification pour utilisation dans l'authentification d'un message d'authentification émis depuis un émetteur vers un récepteur, le moyen de code programme lisible par ordinateur inclut :

un premier moyen de code programme lisible par ordinateur pour amener ledit ordinateur à établir au niveau du côté émetteur une première clé privée procurée par $N \geq 2$ nombres premiers $p_1, p_2, ..., p_N$, une première clé publique n procurée par un produit $p_1{}^{k1}, p_2{}^{k2}, ..., p_N{}^{kN}$, où k1, k2, ..., kN sont des nombres entiers positifs arbitraires, une seconde clé publique e et une seconde clé privée e qui satisfont :

$$ed \equiv 1 \pmod{L}$$

où L est le plus petit commun multiple de p_1-1, p_2-1, ..., p_N-1 ;
un second moyen de code programme lisible par ordinateur pour amener ledit ordinateur à obtenir au niveau du côté émetteur un authentificateur h(M) en hachant le message d'authentification M en utilisant une fonction de hachage h, et
un troisième moyen de code programme lisible par ordinateur pour amener ledit ordinateur à obtenir au niveau du côté émetteur un authentificateur chiffré h(C) de l'authentificateur h(M) en conformité avec :

$$h(M) \equiv h(C)e \pmod{n}$$

en obtenant les résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ..., p_N^{kN}, respectivement, de l'authentificateur chiffré h(C) en utilisant un calcul en boucle par rapport à la première clé privée p_1, p_2, ..., p_N, et en appliquant le théorème de reste chinois aux résidus $h(C)_{p1k1}$, $h(C)_{p2k2}$, ..., $h(C)_{pNkN}$, et en émettant ensuite l'authentificateur chiffré h(C) et le message d'authentification M vers le récepteur :

CARACTERISE EN CE QUE

l'authentificateur chiffré h(C) est obtenu en utilisant la première clé privée procurée par les deux nombres premiers $p_1 = p$ et $p_2 = q$ et la première clé publique n procurée par le produit p^kq où k = k1 ;
le troisième moyen de code programme lisible par ordinateur obtient un résidu $h(k)_0$ modulo p et un résidu $h(C)_q$ modulo q de l'authentificateur chiffré h(C) par des calculs d'exposant modulaire de nombre d'entier de :

$$h(K)_0 := h(M)^{dp} \pmod{p} ;$$

et

$$h(C)_q := h(M)^{dq} \pmod{q} ;$$

où :

$$dp := d \pmod{p-1} ;$$

et

$$dq := d \pmod{q-1} ;$$

et obtient un résidu $h(C)_{pk}$ modulo p^k de l'authentificateur chiffré h(C) en appliquant le calcul en boucle à $h(k)_0$, et applique le théorème de reste chinois aux résidus $h(C)_{pk}$ et $h(C)_q$; et
le calcul en boucle est effectué par :

(a) établir $h(A)_0 = h(K)_0$;
(b) pour i=1 à (k-1) est calculé de manière répétée

$$h(F)_i := (h(A)_{i-1}{}^e) \pmod{p^{i+1}} ;$$

$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}} ;$$

$$h(B)_i := h(E)_i/p^i \text{ dans } Z ;$$

$$h(K)_i := ((eh(F)i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p} ;$$

$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ dans } Z ;$$

et

(c) établir $h(C)_{pk} := h(A)_{k-1}$.

FIG. 1

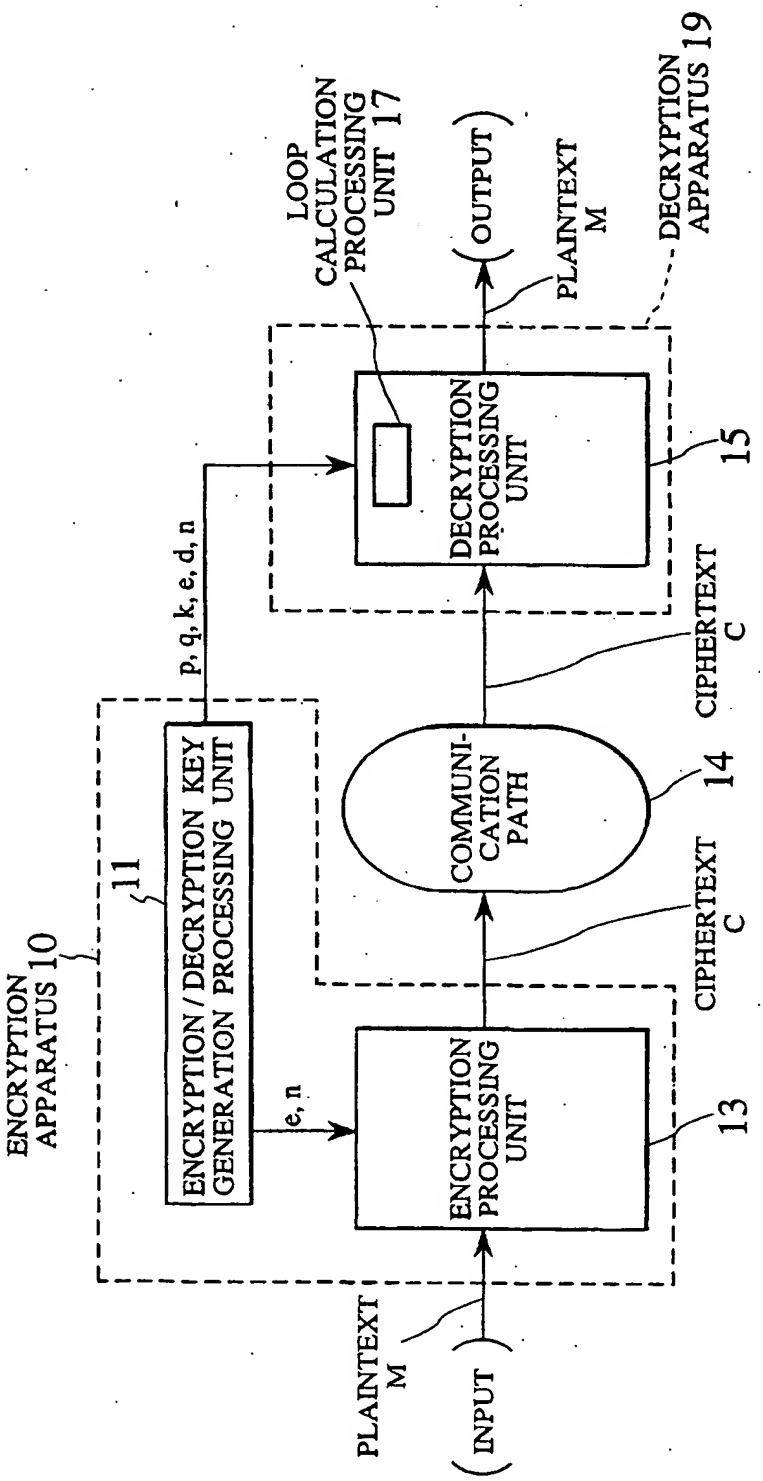

ENCRYPTION APPARATUS 10
11
ENCRYPTION / DECRYPTION KEY GENERATION PROCESSING UNIT
p, q, k, e, d, n
e, n
ENCRYPTION PROCESSING UNIT
13
PLAINTEXT M
(INPUT)
CIPHERTEXT C
COMMUNI-CATION PATH
14
CIPHERTEXT C
DECRYPTION PROCESSING UNIT
15
LOOP CALCULATION PROCESSING UNIT 17
(OUTPUT)
PLAINTEXT M
DECRYPTION APPARATUS 19

FIG. 2

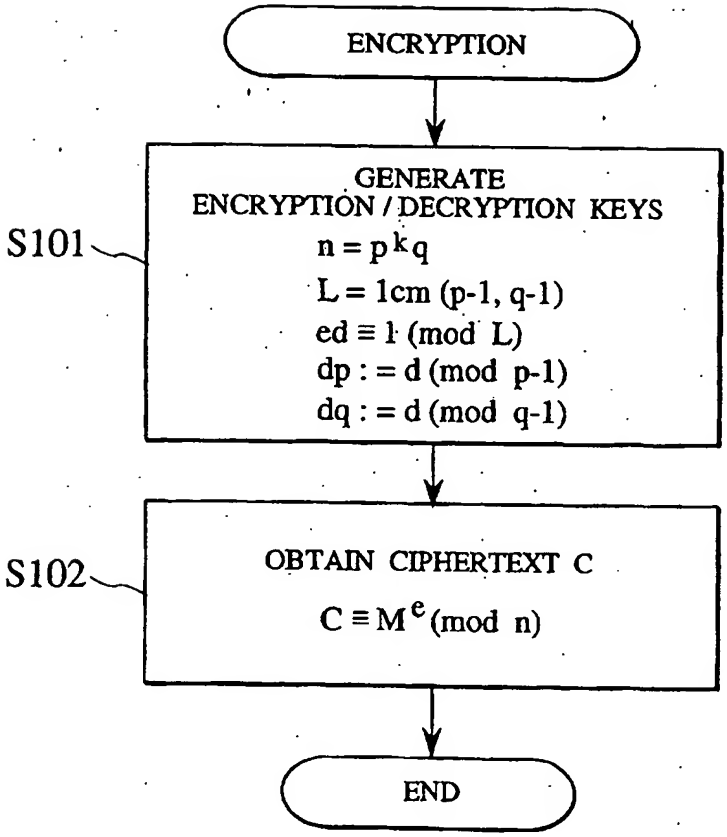

ENCRYPTION
GENERATE
ENCRYPTION / DECRYPTION KEYS
S101
$n = p^k q$
$L = 1cm\ (p-1, q-1)$
$ed \equiv 1 \pmod{L}$
$dp := d \pmod{p-1}$
$dq := d \pmod{q-1}$
OBTAIN CIPHERTEXT C
S102
$C \equiv M^e \pmod{n}$
END

FIG. 3

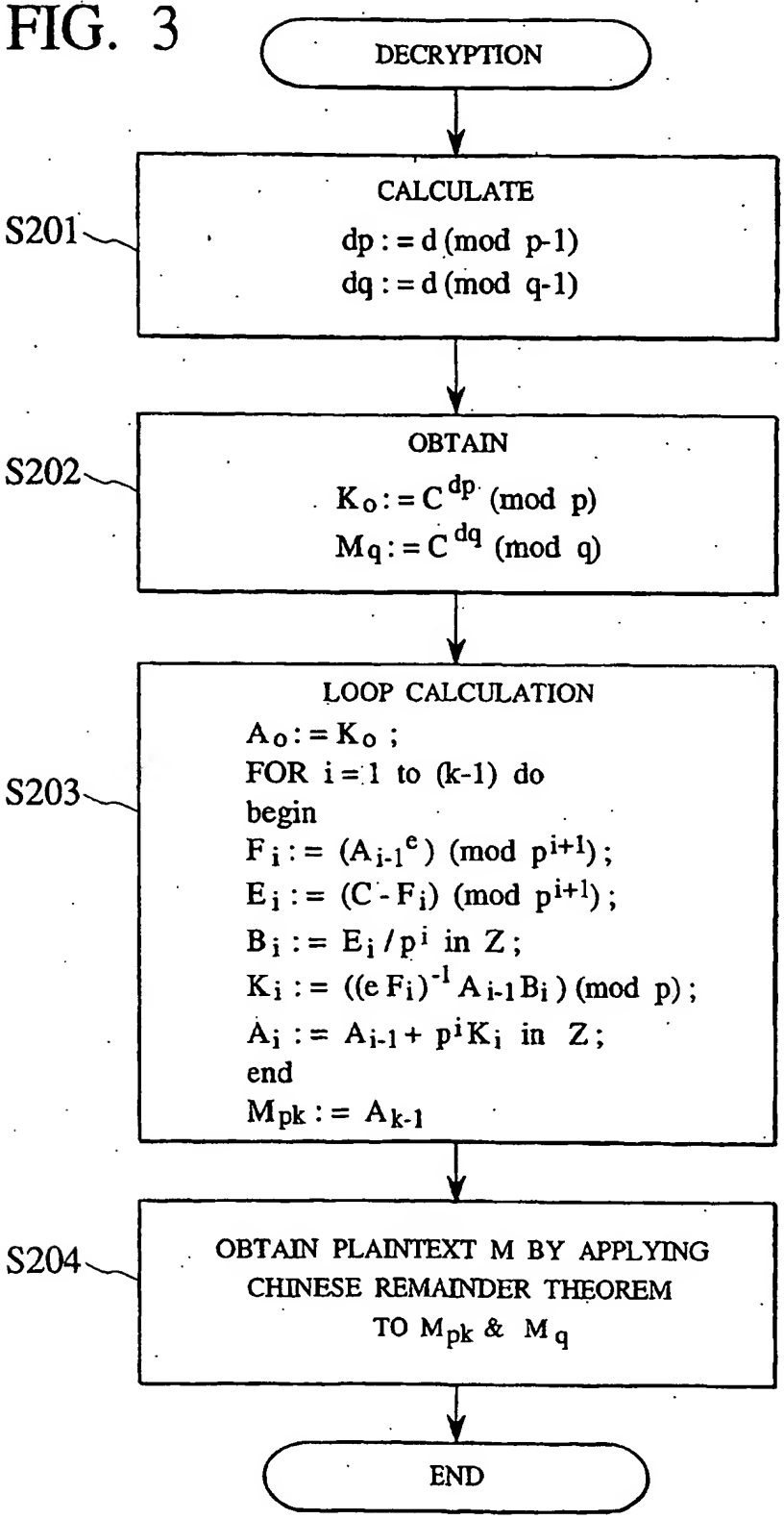

DECRYPTION
S201
CALCULATE
dp : = d (mod p-1)
dq : = d (mod q-1)
S202
OBTAIN
$K_o := C^{dp} \pmod p$
$M_q := C^{dq} \pmod q$
S203
LOOP CALCULATION
$A_o := K_o$;
FOR i = 1 to (k-1) do
begin
$F_i := (A_{i-1}^e) \pmod{p^{i+1}}$;
$E_i := (C - F_i) \pmod{p^{i+1}}$;
$B_i := E_i / p^i$ in Z;
$K_i := ((e F_i)^{-1} A_{i-1} B_i) \pmod p$;
$A_i := A_{i-1} + p^i K_i$ in Z;
end
$M_{pk} := A_{k-1}$
S204
OBTAIN PLAINTEXT M BY APPLYING CHINESE REMAINDER THEOREM TO M_{pk} & M_q
END

FIG. 4

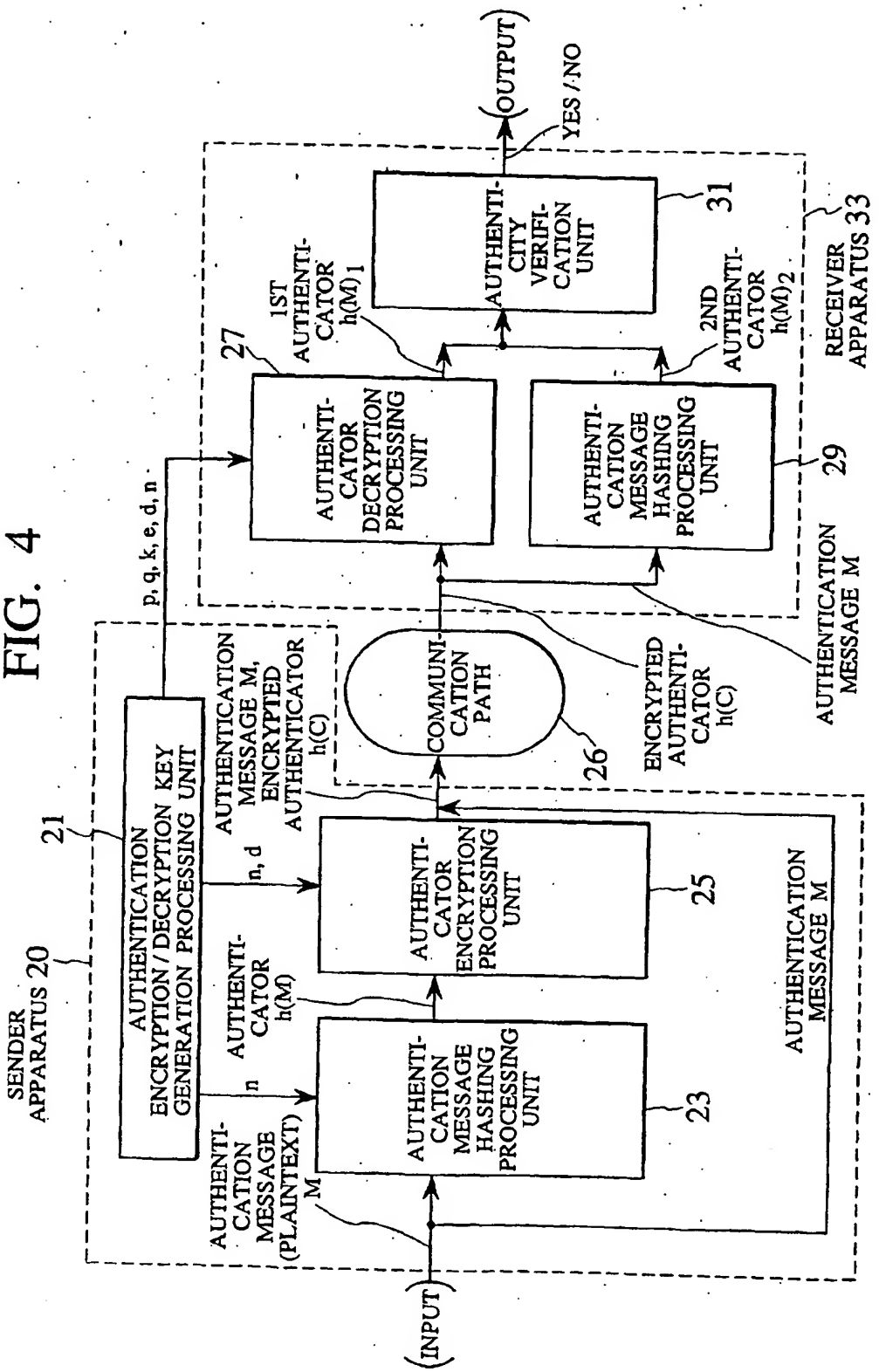
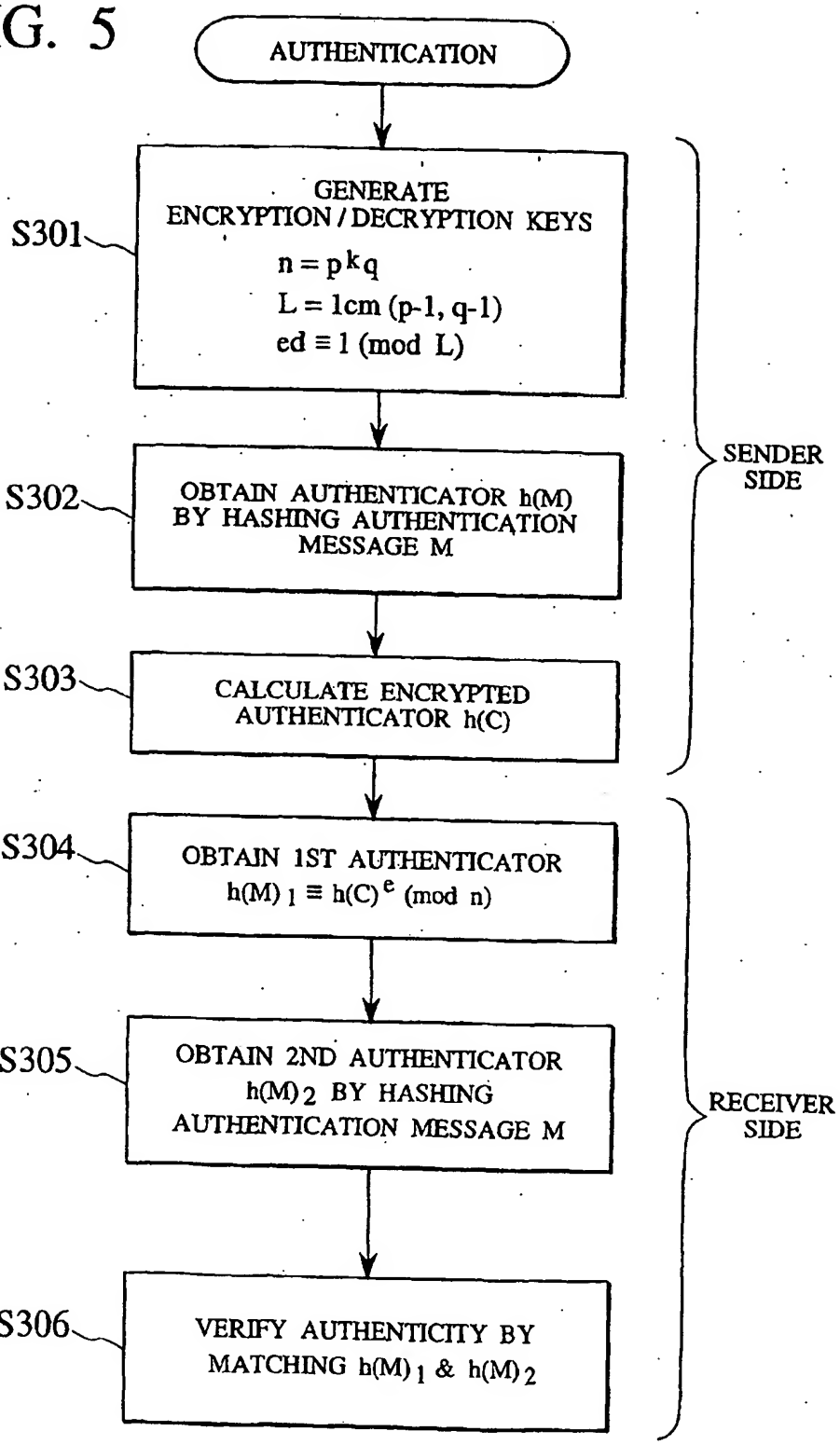

SENDER APPARATUS 20
AUTHENTICATION ENCRYPTION / DECRYPTION KEY GENERATION PROCESSING UNIT
21
p, q, k, e, d, n
AUTHENTICATION MESSAGE M, ENCRYPTED AUTHENTICATOR h(C)
n, d
AUTHENTICATION MESSAGE (PLAINTEXT) M
n
AUTHENTICATOR h(M)
AUTHENTICATION MESSAGE HASHING PROCESSING UNIT
23
AUTHENTICATOR ENCRYPTION PROCESSING UNIT
25
AUTHENTICATION MESSAGE M
COMMUNICATION PATH
26
ENCRYPTED AUTHENTICATOR h(C)
AUTHENTICATION MESSAGE M
RECEIVER APPARATUS 33
AUTHENTICATOR DECRYPTION PROCESSING UNIT
27
1ST AUTHENTICATOR h(M)1
AUTHENTICATION MESSAGE HASHING PROCESSING UNIT
29
2ND AUTHENTICATOR h(M)2
AUTHENTICITY VERIFICATION UNIT
31
YES / NO
(INPUT)
(OUTPUT)

FIG. 5


AUTHENTICATION
S301
GENERATE ENCRYPTION / DECRYPTION KEYS
$n = p^k q$
$L = 1cm\ (p-1, q-1)$
$ed \equiv 1\ (mod\ L)$
S302
OBTAIN AUTHENTICATOR h(M) BY HASHING AUTHENTICATION MESSAGE M
S303
CALCULATE ENCRYPTED AUTHENTICATOR h(C)
SENDER SIDE
S304
OBTAIN 1ST AUTHENTICATOR
$h(M)_1 \equiv h(C)^e\ (mod\ n)$
S305
OBTAIN 2ND AUTHENTICATOR $h(M)_2$ BY HASHING AUTHENTICATION MESSAGE M
S306
VERIFY AUTHENTICITY BY MATCHING $h(M)_1$ & $h(M)_2$
RECEIVER SIDE